



NRL/MR/5540--00-8459

Network Pump (NP) Security Target

ANDREW P. MOORE

*Center for High Assurance Computer Systems
Information Technology Division*

May 29, 2000

Approved for public release; distribution unlimited.

20000605 142

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE May 29, 2000	3. REPORT TYPE AND DATES COVERED Memorandum Report 1/98—4/00	
4. TITLE AND SUBTITLE Network Pump (NP) Security Target			5. FUNDING NUMBERS PE – 20001F	
6. AUTHOR(S) Andrew P. Moore				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Research Laboratory Washington, DC 20375-5320			8. PERFORMING ORGANIZATION REPORT NUMBER NRL/MR/5540--00-8459	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) COMSPAWARSSYSCOM San Diego, CA National Security Agency 9800 Savage Road Ft. Meade, MD 20755			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) This paper describes the security requirements and top level design of a network security device called the Network Pump (NP). The NP provides general purpose, reliable, and secure communications between two system high enclaves operating at different classification levels. This paper is structured as a Security Target as required by the Common Criteria [9].				
14. SUBJECT TERMS Common Criteria Security Target Evaluation Network security One-way flow Boundary controller Guard			15. NUMBER OF PAGES 58	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	

Table of Contents

Chapter 1	Introduction.....	1
1.1	Identification.....	1
1.2	Overview.....	1
1.3	Conformance Claim.....	2
Chapter 2	Network Pump Description.....	3
2.1	Pump Protocol.....	4
2.1.1	Control Messages.....	4
2.1.2	Data Messages.....	4
2.2	Low Wrapper Functions.....	5
2.3	High Wrapper Functions.....	5
2.4	NP Functions.....	5
Chapter 3	Security Environment.....	8
3.1	Threats to be Addressed by NP Operations.....	8
3.1.1	Threat to Confidentiality.....	9
3.1.2	Threat to Integrity.....	9
3.1.3	Threat to Availability.....	9
3.1.4	Threat to Configuration.....	10
3.1.5	Threat to Detection.....	10
3.2	Threats to be Addressed by the Low and High LAN Environments.....	10
3.2.1	Threat to Integrity.....	11
3.2.2	Threat to Availability.....	11
Chapter 4	Security Objectives.....	12
4.1	NP Technical Security Objectives.....	12
4.2	NP Non-Technical Security Objectives.....	13
4.3	Security Objectives Rationale.....	13
Chapter 5	Security Requirements.....	16
5.1	Security Functional Requirements (SFR).....	16
5.1.1	Requirements for Security Audit (FAU).....	17
5.1.2	Requirements for Data Protection (FDP).....	18
5.1.3	Requirements for Identification and Authentication (FIA).....	19
5.1.4	Requirements for Security Management (FMT).....	19
5.1.5	Requirements for Protection of the TOE Security Functions (FPT).....	20
5.1.6	Requirements for Resource Utilization (FRU).....	21
5.1.7	Requirements for TOE Access (FTA).....	21
5.1.8	Requirements for Trusted Path/Channels (FTP).....	21
5.1.9	Minimum Strength of Function Levels.....	22
5.2	Security Functional Requirements Rationale.....	22
5.2.1	Satisfaction of Objective O1.....	23
5.2.2	Satisfaction of Objective O2.....	23
5.2.3	Satisfaction of Objective O3.....	23
5.2.4	Satisfaction of Objective O4.....	24
5.2.5	Satisfaction of Objective O6.....	24
5.2.6	Satisfaction of Objective O7.....	24
5.2.7	Satisfaction of Objective O8.....	24
5.2.8	Satisfaction of Objective O9.....	24
5.2.9	Satisfaction of Objective O10.....	25
5.2.10	Strength of Function Requirement Consistency.....	25
5.2.11	Security Requirements Mutually Supportive.....	25
5.3	NP Security Assurance Requirements.....	28
5.3.1	Requirements for Configuration Management (ACM).....	29
5.3.2	Requirements for Delivery and Operation (ADO).....	30
5.3.3	Requirements for Development (ADV).....	30
5.3.4	Requirements for Guidance documents (AGD).....	33

5.3.5	Requirements for Life Cycle Support (ALC).....	34
5.3.6	Requirements for Tests (ATE).....	35
5.3.7	Requirements for Vulnerability Assessment (AVA)	36
Chapter 6	Summary Specification.....	38
6.1	Security Functions (SF)	38
6.1.1	Functions for Confidentiality	38
6.1.2	Functions for Integrity	39
6.1.3	Functions for Identification and Authentication	39
6.1.4	Functions for Availability	40
6.1.5	Functions for Administrative Provision.....	40
6.1.6	Functions for Administrative Control	41
6.1.7	Functions for Security Audit.....	41
6.1.8	Functions for Self-Test	42
6.1.9	Functions for Secure Failure and Recovery	42
6.2	Security Function Rationale.....	43
6.2.1	Confidentiality Argument	44
6.2.2	Integrity Argument	45
6.2.3	Identification and Authentication Argument	45
6.2.4	Connection Control Argument.....	46
6.2.5	Availability Argument	46
6.2.6	Administrative Provision Argument	46
6.2.7	Administrative Control Argument	47
6.2.8	Security Audit Argument.....	47
6.2.9	Self-Test Argument.....	47
6.2.10	Secure Failure and Recovery Argument	47
6.2.11	Non-Bypassability Argument	48
6.2.12	Domain Separation Argument	48
6.2.13	Strength of Function Levels for Security Functions	48
References	50
Appendix A	51

Table of Tables

Table 1: Secure Usage Assumptions	8
Table 2: Threats to be Addressed by NP Operations	9
Table 3: Threats to be Addressed by the Low and High LAN Environments	10
Table 4: NP Technical Security Objectives	12
Table 5: NP Non-Technical Security Objectives	13
Table 6: Security Threat/Objective Cross-Reference	14
Table 7: The NP's Security Functional Requirement Classification	17
Table 8: Security Objective/Functional Requirement Cross-Reference	23
Table 9: Dependency Analysis	26
Table 10: SFR Mutual Support.....	27
Table 11: Assurance Requirement Components for EAL5.....	29
Table 12: Security Functional Requirement/Security Function Cross-Reference	44

Table of Figures

Figure 1: The System Architecture with the NP.....	3
Figure 2: Structure of a Wrapper	3
Figure 3: States of a NP Connection.....	38

Network Pump (NP) Security Target

Chapter 1 Introduction

1.1 Identification

Target of Evaluation: Network Pump

Product Type: Low to High Network Communication Link

Developer:

Center for High Assurance Computer Systems, Code 5540
Naval Research Laboratory
Washington, D.C.

Sponsor:

Space and Naval Warfare Systems Command, PD-161
San Diego, CA

Version: Hardware Pump

Keywords:

MLS guard, one-way link, Low to High flow, reliable communication, MLS information sharing, covert channel analysis, information theory, high assurance

1.2 Overview

Many DoD computer systems are, for reasons of security, operated in System High enclaves. This organization permits free flow of information and arbitrary system connectivity within an enclave operating at a single security level, but makes it risky to connect enclaves operating at different security levels.

If the security levels of two enclaves are, respectively, Low and High, and High dominates Low in the lattice of security levels, then communication from Low to High can be safely permitted, but communication from High to Low must be restricted. If communication from High to Low is prohibited entirely, reliable transmission from Low to High becomes extremely difficult, and most conventional computer communication protocols cannot function normally.

This Security Target describes a Target of Evaluation called the Network Pump (NP) [1,3]. The NP provides general purpose, reliable and secure communication between two System High enclaves operating at Low and High. While other such devices provide a single connection between a single device operating at Low and another at High, the NP provides multiple, simultaneous connections between users of one LAN operating at Low and users of another LAN operating at High. To be most useful, the NP must provide

1. high assurance that significant information will not leak from the High network to the Low network, so that networks operating at substantially different security levels can be securely connected,
2. high assurance that a message accepted by the NP from Low will eventually be delivered to the intended High recipient, even in the face of power failures or system crashes,
3. high performance, so that information can normally be passed quickly and many connections can be supported,

4. flexible interfaces, so that it can support communication needs of many different applications, and
5. low initial and operating costs, so that expense will not be a barrier to deployment.

The NP's primary security objective is to preserve the confidentiality of High information. While this may not at first seem to be a problem with a Low to High communication link, consider the simple case of a Store and Forward Buffer (SAFB) used to transmit messages from Low to High. Reliability requires sending an acknowledgement to Low for each message received that guarantees that the SAFB will forward the message to High. When the SAFB is full, the timing of these acknowledgements is directly under the control of High and thus, if maliciously exploited, represents a covert timing channel. That is, a High side process controlled by a malicious user or code, e.g., a Trojan Horse program, can encode High information by varying the acknowledgement arrival times to Low, after Low has sent a message to High. A colluding Low side process that decodes this information breaches the confidentiality of the High information. Other work [8] demonstrates that such covert channels have significant capacities in real systems. The NP described in this Security Target permits connecting Low and High LANs while providing high assurance that confidentiality is preserved by severely constraining the capacity of channels from High to Low.

1.3 Conformance Claim

The NP, as described in this document, contains only functional requirements that are based upon functional components in Part 2 of the Common Criteria. In addition this document mandates the EAL5 level of assurance, with no additional assurance requirements. The NP is, therefore, Part 2 and Part 3 conformant, as defined by the Common Criteria.

Chapter 2 Network Pump Description

The general architecture in which the NP resides is shown in Figure 1. The NP supports communication connections from the Low LAN Interface to the High LAN Interface. These connections may support random traffic, e.g., e-mail, from the Low to High or more structured updates of High LAN databases, e.g., SQL updates that replicate Low LAN database updates to the High LAN. The NP supports a specialized protocol, called the *Pump Protocol*, across the LAN interfaces for ease of re-use and maintenance. The NP operates compatibly with protocols from the TCP/IP suite [4]. TCP/IP is usually described as supporting four layers (listed from lowest to highest): network access layer, internet layer, host-host transport layer, and application layer. The *Pump Protocol* is implemented at the application layer and uses the services provided by the transport layer.

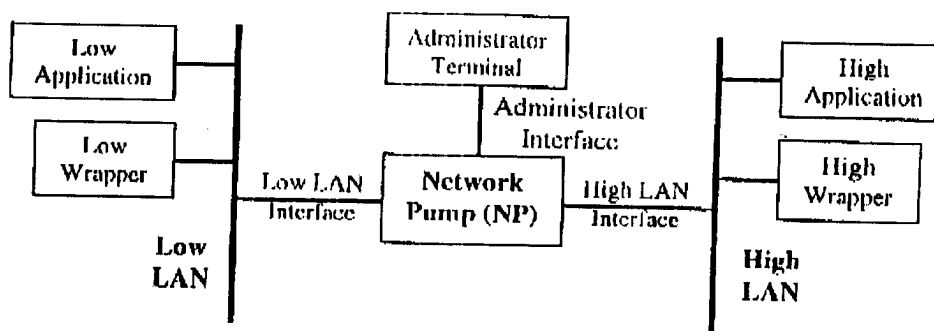


Figure 1: The System Architecture with the NP

The ability to support a variety of applications is provided by components called *wrappers*. These components run on the application systems in the Low and High enclaves that communicate with the NP over their respective LANs. Each application on the Low LAN that uses the NP communicates via an interface to a Low Wrapper, and, similarly, each application on the High LAN that receives information from the Pump communicates via an interface to a High Wrapper. The wrappers are responsible for supporting the *Pump Protocol* on one side and the particular application protocol on the other. Different wrappers will support different applications; installing or modifying a wrapper is a change to the software configuration on the application system, but not to the NP.

As shown in Figure 2, each wrapper is further divided into an application-dependent part, which can be tailored to support the particular set of objects, or calls the application expects to see, and a Pump-dependent part, which is a library of routines that implement the *Pump Protocol* [5]. These functions can be called as required by the application-dependent routines.

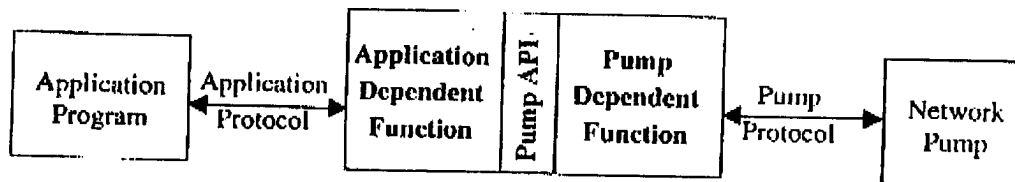


Figure 2: Structure of a Wrapper

The Pump also provides the interface to an Administrator Terminal. The Pump receives initial configuration and other control information across this interface and provides error and performance reports, if requested by the Administrator. The configuration information defines which users on the

Low LAN are permitted to open connections (and thereby transmit messages) to which users on the High LAN.

2.1 Pump Protocol

The *Pump Protocol* is a special-purpose protocol implemented at the application layer [4] that defines the communications at this level between the NP and the Low Wrapper and High Wrapper. The protocols used below the application layer (transport, internet, and network interface layers) must support communication across Ethernet LANs. The *Pump Protocol* is specified in terms of the messages it transmits. There are two classes of messages: Control Messages and Data Messages.

2.1.1 Control Messages

Control Messages support the creation and termination of connections. There are three types of control messages:

1. **Request Connection:** This message specifies the desired source and destination of the connection as an IP address and port number and specifies whether a recoverable or non-recoverable connection is desired. It is sent from the Low Wrapper to a well-known port on the NP.
2. **Connection Valid/Invalid:** This message is sent from the NP to a Low Wrapper in response to a Request Connection Message. If the message indicates a connection is invalid, it implies that the requested connection is not consistent with the Configuration Table or that the host is unavailable. If the requested connection is valid, the Low Wrapper is expected to listen for a Connection Granted message.
3. **Connection Granted:** This message is sent from the NP to a Low Wrapper following a Connection Valid message and indicates that the Low Wrapper can begin sending messages across the connection. The same message is also sent to the High Wrapper at the IP address and port specified in the connection request. It also provides communication parameters for the connection, including Connection ID, maximum message size, window size, and initial time out value. If the requested connection was recoverable, and the previous connection between this pair of IP/port addresses was both recoverable and terminated abnormally within the past 24 hours, then the last message transmitted to High Wrapper across the previous connection is appended to this control message.
4. **Connection Exit:** This is a message sent by the NP to the High Wrapper and Low Wrapper to indicate that an existing connection is being terminated abnormally. It is to be sent when an Administrator requests that a connection be closed or when the NP detects an abnormal condition on a connection (e.g., High Wrapper ceases to accept messages, Low Wrapper ceases to send messages).

2.1.2 Data Messages

Data Messages support the flow of messages and acknowledgments across an existing connection and can also indicate the normal termination of a connection.

1. **Data Message (Low to High):** This protocol unit transmits a single, non-zero-length message from Low Wrapper to High Wrapper over the connection specified by a connection ID. The sender of a Data Message also provides a Message ID, which can act as a sequence number. This Data Message is sent from the Low Wrapper to the NP and, subsequently, from the NP to the High Wrapper.
2. **Acknowledgment (High to Low):** This protocol unit acknowledges receipt by the sender of a message, specified by a Message ID, over a connection, specified by a Connection ID. The NP will send a message of this type to the Low Wrapper after it successfully receives a Data Message from the Low Wrapper. The High Wrapper will send a message of this type to the NP whenever the High Wrapper successfully receives a Data Message from the NP.
3. **Close Connection Message:** This protocol unit is sent from the Low Wrapper to the NP, and subsequently from the NP to the High Wrapper to terminate a connection normally. It specifies a Connection ID.

2.2 Low Wrapper Functions

The Low Wrapper shall include an application-dependent part and Pump-dependent part. The Pump-dependent part of the Low Wrapper shall provide the following functions to the application-dependent part by invoking appropriate *Pump Protocol* operations:

1. **Request Connection:** The application specifies the desired destination and connection type.
2. **Send Data:** The application requests data to be sent over an existing connection.
3. **Close Connection:** The application signals that it has no more data to transmit.

The application-dependent part of the Low Wrapper will map application communication requirements into these functions as needed. The Pump-dependent part of the Low Wrapper may return information to the application-dependent part in response to each of these operations (for example, the connection request may be accepted or refused, and an acknowledgment may be returned after data are sent). Whether this information is conveyed by the application-dependent part back to the Low Application will depend on the Low Application's requirements.

2.3 High Wrapper Functions

The High Wrapper shall include a Pump-dependent part and an application-dependent part. The Pump-dependent part shall provide the following functions:

1. **Receive Connection:** This function returns the information provided by the Connection Granted message to enable initialization of data structures for a new connection.
2. **Receive Message:** This function returns the next message received from the NP for the connection that corresponds to this High Wrapper
3. **Send Acknowledgment:** This function transmits an Acknowledgment to be transmitted over the specified connection for a specified message.

The application-dependent part of the High Wrapper will map application communication requirements into these functions as needed. The Pump-dependent part of the High Wrapper may return information to the application-dependent part in response to each of these operations (for example, the Pump may terminate a connection, causing an abnormal return from the requested operation). Whether this information is conveyed by the application-dependent part back to the High Application will depend on the High Application's requirements.

2.4 NP Functions

The fundamental function of the NP is to provide reliable transmission of information from the Low LAN to the High LAN while ensuring that High information cannot leak to the Low LAN. Confidentiality properties of the NP depend solely on the NP itself and not on the Wrappers. Wrapper function, including both application-dependent and Pump-dependent parts, is not confidentiality critical and can be altered or replaced without affecting system confidentiality. The confidentiality critical nature of NP function stems from the ability of a High user/process to control the timing of application-layer acknowledgements, as in the case of the Store and Forward Buffer when the buffer is full.

The NP ensures that communication over the LAN Interfaces conforms strictly to the *Pump Protocol*; any other application-level traffic is logged as erroneous and discarded. The NP controls the timing of the acknowledgments sent across the Low LAN interface, and thus the covert timing channel, according to an algorithm provided in reference [1]. This algorithm bounds the capacity of the covert channel analytically as follows:

For each active connection, the NP maintains a separate variable that reflects the moving average of the time it takes the High Wrapper to accept messages from the High LAN Interface. The NP delays application-layer acknowledgments, which are sent in response to messages received from the Low Wrapper over this connection, randomly according to

this moving average. At the application layer, messages received over this connection shall be acknowledged in the same order they are received. The only information flow from the High Wrapper to the Low Wrapper over a connection occurs through changes in the value of the moving average variable. This variable shall not be provided directly to the Low Wrapper but the Low Wrapper may estimate its value by observing the randomized delays between message transmission and receipt of acknowledgments.

The NP supports the functions of the *Pump Protocol* and Administrator Terminal requests as follows:

1. The NP responds to a Request Connection control message received from a Low Wrapper over the well-known port designated for this purpose by checking the request against the Configuration Table and, if the request is invalid, sending a Connection Invalid message to the Low Wrapper. If the request is valid, a Connection Valid message is sent, and a Connection ID is allocated for this connection. The NP then constructs a Connection Granted message containing appropriate data for this connection. If the request is valid and recoverability is requested, the NP also check to see whether the previous connection between the requested sender and receiver was terminated abnormally. If so, it returns the last message successfully transmitted from Low to High on that connection to the Low Wrapper along with the Connection Valid message.

2. The NP responds to a Data Message from the Low Wrapper by checking that the specified connection is valid and that the message fits the connection's parameters.

If the connection is valid, and there is space available in the NP Buffer, it stores the message in the NP Buffer, generates an acknowledgment delay based on the current value of the moving average for this connection and a random factor in accordance with the NP algorithms [KML 96]. After this delay elapses, the NP transmits the appropriate acknowledgment to the Low Wrapper.

If space is not available in the NP Buffer, the NP will generate a timeout event for itself. If space becomes available in the NP Buffer prior to the occurrence of the timeout, the message will be handled as in the preceding paragraph, except that the random delay computed for the acknowledgment will be modified to take into account the time elapsed between the receipt of the message and its placement in the buffer. If the timeout occurs before space becomes available, the message is discarded without sending an acknowledgment, since the Low Wrapper, not having received an acknowledgment, will retransmit the message.

3. The NP responds to a Close Message from the Low Wrapper by forwarding that message to the High Wrapper freeing the data structures allocated to this connection, and recording the connection as having terminated normally.
4. The NP responds to an Acknowledgment received from the High Wrapper on a given connection by updating the value of the moving average for this connection appropriately and releasing all storage associated with this message. If this is a recoverable connection, the NP places the message corresponding to the acknowledgment in the "last successfully transmitted message" stable storage buffer for this connection prior to releasing the storage associated with this message.
5. The NP terminates any protocol operation that takes longer than the configured Network Inactivity Timeout Value to return a result. Following such a termination, the NP logs the fact of the termination and continues as if a Connection Exit request had been received from the Administrator Terminal to terminate this connection (see item 6 below).
6. The NP responds to a Connection Exit request from the Administrator Terminal by releasing temporary storage related to this connection, and, if it is a recoverable connection, marking the connection as abnormally terminated in a data structure that can be consulted the next time a connection between the same sender/receiver pair is requested.
7. The NP responds to a Load Configuration request received from the Administrator Terminal by immediately replacing the existing Configuration Table with the new Table. The Configuration table specifies general parameters such as window sizes, buffer sizes, time out periods, maximum connections per host, maximum connections per Pump, the IP addresses and port numbers on the Low LAN from which the NP will accept connection requests and messages whether a particular IP address/port requires recoverable service, the IP addresses and port numbers on the High LAN to which the NP will

deliver messages, and which of the Low addresses is authorized to send to which of the High addresses.

8. The NP responds to a Retrieve Status request from the Administrator Terminal by returning the Configuration Table and the current contents of auditing and error-logging data structures. Status information includes error reports, such as the number of erroneous messages received and number of improper connections attempted since the last report, and performance data, such as the number of connections initiated, number of messages successfully transmitted per connection, average delay per message, and current moving average values.
9. The NP responds to a Renew Status request by both returning the current status information and resetting all counters and status indicators to their initial states, except for the system clock. The NP releases any messages saved from abnormally terminated conditions that are older than 24 hours in response to this request.

The NP maintains the following characteristics while implementing the functions of the *Pump Protocol*:

Throughput: The NP supports a minimum average data throughput of 2 megabits per second, from Low Wrapper to High Wrapper. On average, the NP can receive data on a particular connection from the Low Wrapper at the same rate that the High Wrapper for that connection accepts data from the NP.

Recoverability: The NP provides recoverable service. That is, once Low Wrapper receives an application layer acknowledgment from the NP for a given message, it can safely assume that the message will be delivered to the High Wrapper by the NP, even if power failures or system crashes occur, either in the NP or the High Wrapper.

Accuracy and Validity: The NP and Wrappers do not degrade the accuracy or validity of any applications to which they are connected. Each message delivered to a High Application by the High Wrapper over a given connection corresponds exactly to a message received from the Low Application by the Low Wrapper.

Message and Acknowledgment Ordering: For each message received successfully by the NP from a Low Wrapper over a connection, the NP sends an acknowledgment message back to the Low Wrapper over the same connection, and the acknowledgments are sent in the same order that the messages are received. The NP delivers messages to the High Application by the High Wrapper in the same order they are received from the Low Application by the Low Wrapper. (Note that these requirements apply at the application protocol layer and do not preclude the use of lower level protocols that may permit subdividing messages into packets, packet duplication, out-of-order delivery of packets, packet retransmission, etc., over both the High LAN and Low LAN interfaces).

Non-Duplication of Messages: The NP successfully delivers each data message successfully received from the Low Wrapper to the High Wrapper exactly once, for recoverable connections, and at most once, for non-recoverable connections.

Connection Independence: Abnormal behavior (such as message flooding or refusal to accept messages) on one connection will not affect the performance of other connections.

Connection Fairness: Connections that are behaving normally receive service on a fair basis.

Chapter 3 Security Environment

To provide a complete picture of the security problem, the Common Criteria requires enumeration of all threats to the NP environment, including those not completely addressed by the NP. Since the NP needs to be useful for many types of environments, we assume a broad range of threats to the NP environment, including threats to information confidentiality, integrity, and availability. This chapter refines these general threats into threats that the NP will address and those that the NP's operating environment will address. Table 1 describes the assumptions on which these threats are based, in the context of Figure 1.

A1. The NP interconnects with the Administrator Terminal, Low LAN, and High LAN as shown in Figure 1.

A2. High dominates Low in the lattice of security levels.

A3. Only personnel cleared for Low information can access data stored on the Low LAN including data transmitted on the Low LAN Interface.

A4. Only personnel cleared for High information can access data stored on the High LAN including data transmitted on the High LAN Interface.

A5. All data received by the NP over the Low LAN Interface are classified Low.

A6. All data received by the NP over the High LAN Interface are classified High.

Table 1: Secure Usage Assumptions

3.1 *Threats to be Addressed by NP Operations*

Table 2 describes the threats addressed by the NP using both technical and non-technical countermeasures. Thus, the NP device implementation may not entirely address the threats listed here; countering them may depend on Physical, Personnel and/or Operational countermeasures in the environment. The next chapter will distinguish the security objectives that derive from these threats as to whether they are addressed by the NP implementation, i.e., by technical countermeasures, or by the NP's environment, i.e., by non-technical countermeasures.

- T1.** High information leaks through the NP to the Low LAN Interface.
- T2.** The integrity of user data received over the Low LAN Interface is compromised as it is transmitted to the High LAN Interface.
- T3.** An unauthorized Low user/process uses NP connection services to send bogus information to the High LAN Interface.
- T4.** An unauthorized user/process uses an NP connection preventing its use by an authorized user.
- T5.** An authorized High user/process that has access to an NP connection is denied fair use of NP connection services.
- T6.** The NP is improperly configured permitting a breach in security.
- T7.** The audit of security relevant events during NP operation does not permit the discovery and termination of malicious activity.

Table 2: Threats to be Addressed by NP Operations

3.1.1 Threat to Confidentiality

The NP provides users of the High LAN with a means to access information stored on the Low LAN via multiple, simultaneous, and reliable communication connections. The price of this added capability is the need to address the threat to the confidentiality of High information, which is identified as T1 in Table 2. Given A1 and A2, the NP compromises the confidentiality of High information if and only if this threat is exploited. Assumptions A3, A4, and A6 limit the damage of such a breach to the compromise of High data to personnel cleared for Low. Assumption A5 ensures that we don't need to worry about nonsense cases like High information sent over the Low LAN Interface. Likely threat agents are malicious (Trojan Horse) processes on the High LAN or in the NP itself that collude with Low LAN processes/users to leak High information. The NP is exclusively responsible for countering confidentiality attacks that exploit the communication link that it provides.

3.1.2 Threat to Integrity

Threats to the integrity of Low information sent to the High LAN are especially detrimental where mission critical function depends on the accuracy of that information. The NP's role, threat T2, is to counter attacks on the integrity of the Low information under its control. Given A1, the NP may compromise the integrity of the user data received over the Low LAN Interface if that data is corrupted, duplicated, deleted or lost before being successfully transmitted to the High LAN. The most likely threat agent is simply an erroneous NP process, although malicious Low LAN users may try to sabotage NP operation to cause loss of data.

The integrity of Low information sent to the High LAN also depends on restricting use of NP connection services to authorized users. Malicious use of NP connection services, as threat T3 allows, permits corrupting the information on which the High LAN depends. The NP can only address the threats by unauthorized users, not malicious authorized users. Likely threat agents include malicious Low LAN users that spoof any identification mechanisms, e.g., IP address spoofing, or erroneous NP processes that permit unauthorized use of connection services.

3.1.3 Threat to Availability

The NP addresses two threats to the availability of Low information on the High LAN. Threat T4 involves unauthorized use of an NP connection that locks out its authorized use. A malicious

user/process may exploit this threat by using all available NP connections to send bogus traffic while authorized users wait indefinitely for a connection. Threat T5 involves a High user/process that has access to an NP connection, but gets degraded (or no) service over that connection. Such degradation may arise when other users monopolize the NP's communication bandwidth, either maliciously or inadvertently. Likely threat agents include malicious or unreliable NP users/processes and malicious (perhaps unauthorized) Low LAN users that get more than their fair share of NP connection resources.

3.1.4 Threat to Configuration

Improper configuration of the NP (T6) may lead to fairly transparent security vulnerabilities. Parameters of the configuration may be confidentiality relevant (e.g., the number of intervals used to compute the moving average, the maximum number of Connection Request retries, and the re-connect frequency), integrity-relevant (e.g., the enabling of message authentication and the set of valid IP addresses) or availability relevant (e.g., the buffer's fair size, the connection table, the maximum number of simultaneous connections). If set improperly, a significant amount of High information may leak to the Low LAN, High information may be corrupted by bogus Low information, or service denied to legitimate High users. Assuming attacks from the Low LAN Interface are not possible, likely sources of the threat are malicious users/processes on the High LAN or in the NP itself.

3.1.5 Threat to Detection

An audit of security-relevant events is necessary since the risk of a breach of security cannot be eliminated completely [6]. Auditing the appropriate events is a necessary precursor to detecting potential security compromises. An attacker wishing to conceal attempted security violations may try to interfere with the audit process or change the audit logs to prevent discovery, which leads to threat T7. Assuming attacks from the Low LAN Interface are not possible, likely sources of the threat are malicious or unreliable users/processes on the High LAN or in the NP itself.

3.2 Threats to be Addressed by the Low and High LAN Environments

Table 3 identifies threats to the security of the Low and High LANs that are relevant to NP operation. These threats must be addressed to preserve the integrity and availability of Low information on the High LAN.

- TE1. A user/process of the Low LAN authorized to use NP connection services transmits incomplete or inaccurate Low information to High LAN through the NP.
- TE2. A user/process of the High LAN inaccurately or incompletely updates High information given the Low information received from the NP.
- TE3. A user/process of the Low LAN authorized to use NP connection services transmits traffic, e.g., malicious code, through the NP that degrades the performance of the High LAN or one of its components.
- TE4. A user/process of the High LAN that has a legitimate need to use NP connection services to access Low information is denied access to a connection.
- TE5. A user/process of the High LAN needs information from the Low LAN faster than can be provided by the allocated share of the NP's communication bandwidth.

Table 3: Threats to be Addressed by the Low and High LAN Environments

3.2.1 Threat to Integrity

Threats TE1 and TE2 combine with threat T2 to characterize completely the threat to the integrity of the update of High information with Low information transmitted through the NP from the Low LAN. TE1 deals with the integrity of the information sent to the NP, whereas TE2 deals with the integrity of the updates to High information based on the information received from the NP. Addressing these threats requires ensuring the correctness of the mechanisms that relay Low information to the NP and that receive and update High information based on information received from the NP

3.2.2 Threat to Availability

Threats TE3, TE4, and TE5 combine with threats T4 and T5 to characterize completely the threat to the availability of the NP connection service for accessing Low information on the High LAN. The availability threat breaks into the threat that

- the High user cannot access an NP connection due to its unauthorized use (T4),
- the High user cannot access an NP connection due to its authorized use (TE4),
- the NP provides only degraded service to certain connections (T5),
- even though the NP provides full service, the High user cannot access Low information fast enough over a connection (TE5), and
- the Low user degrades performance on the High LAN by what it transmits (TE3).

Threat TE5 may be due to an insufficient communication bandwidth provided by the NP or slow transmission of Low information to the NP by a Low user/process.

Addressing threats TE3, TE4, and TE5 requires an analysis of the High LAN to determine the number and demand rate of connections needed by High users/processes. Traffic received from the NP may have to be screened, e.g., for viruses, before being made available. This process combined with limitations on the NP's throughput must not slow the update process down to a point unacceptable to High LAN users. Multiple NPs can be used if needed to increase the number of connections available and their effective throughput per connection.

Chapter 4 Security Objectives

This chapter describes how the NP addresses the threats identified in the previous chapter. Section 4.1 identifies the technical security objectives that the NP implementation requires. Section 4.2 describes non-technical objectives of the NP environment that support the technical objectives. Finally, Section 4.3 explicitly traces the security objectives back to the threats that they address.

4.1 NP Technical Security Objectives

The technical security objectives for the NP, which are listed in Table 4, derive from the overall goals of confidentiality, integrity and availability. These objectives define precisely the NP's support for achieving each of these goals in the environment in which it is to be embedded.

- O1.** The NP must prevent overt channels that transmit High information to the Low LAN Interface
- O2.** The NP must constrain the capacity of covert storage and timing channels that leak High information to the Low LAN Interface according to configuration settings.
- O3.** The NP must ensure that information sent to the High LAN Interface accurately represents information received over the Low LAN Interface.
- O4.** The NP must identify and authenticate individuals/processes before permitting access to any other NP functions.
- O5.** The NP must ensure that only authorized users may access the NP connection services.
- O6.** The NP must ensure that users with access to NP connection services are given a fair share of the communication bandwidth.
- O7.** The NP must provide function that enables an authorized administrator to effectively manage the NP configuration.
- O8.** The NP must ensure that only authorized administrators may access the administrative functions and data.
- O9.** The NP must record the appropriate security relevant events, so that an administrator can detect attacks or misconfiguration that would leave the NP susceptible to attack.
- O10.** The NP must ensure that users can be traced to the security relevant actions in which they engage.

Table 4: NP Technical Security Objectives

The first two objectives deal with the confidentiality of High information by restricting loss to specifically identified covert channels that are appropriately constrained. Objectives O3 and O5 deal with the integrity of information, which is protected from corruption by internal processes or by unauthorized Low users/processes. O5 and O6 deal with the availability of NP connections, to only authorized users, and the availability of the communication bandwidth to those connections. The administrative objectives found in O7 and O8 permit the proper configuration of the NP needed to meet the confidentiality, integrity and availability objectives. Likewise, the audit objectives of O9 and O10 permit detecting, and subsequently

preventing, attacks or misconfiguration that lead to breaches of these objectives. Finally, O4 requires ensuring that users are who they say they are, a foundation for any secure system.

4.2 NP Non-Technical Security Objectives

Table 5 lists the non-technical security objectives that support the technical solution implied in the previous section. Objective OE1 deals with the administrative personnel, OE2 with the NP's physical protection, and OE3 and OE4 with the operational requirements on the authentication data and storage media.

- OE1.** The NP environment must ensure that one or more authorized administrators are assigned who are competent/trustworthy
 - to properly manage the NP configuration (in part, as shown Figure 1) including its connectivity with the environment (as characterized by the Secure Usage assumptions),
 - to define the parameters of the configuration (e.g., constraints on the cover channels permitted), and
 - to review security audit logs to uncover and, subsequently prevent, malicious activity (see also security assurance family ADG_ADM).
- OE2.** The NP environment must physically protect the NP from unauthorized modification during development, delivery, installation and usage (see also security assurance families ALC_DVS, ADO_DEL, and ADO_IGS).
- OE3.** The NP environment must ensure that authentication data is distributed only to authorized users and, once distributed, that users and administrators protect secrets (e.g., passwords, private keys) from disclosure to unauthorized individuals.
- OE4.** The NP environment must properly manage the NP storage media to protect against failure leading to loss or corruption of NP data, including authentication, configuration, audit and user data.

Table 5: NP Non-Technical Security Objectives

4.3 Security Objectives Rationale

Table 6 below cross-references the NP-addressed threats, identified in Section 3.1, against the IT security objectives, identified in Section 4.1. Arguments following the table describe why the identified objectives address the NP threats. The administrator guidance documentation will require NP configuration and environment connections in accordance with the secure usage assumptions as in OE1.

All of the threats addressed by the NP depend on satisfying the security objectives for the environment. This is primarily due to the fact that security (as defined by the security objectives) can be compromised if the security critical data entrusted to the administrator is corrupted. The arguments following the table, therefore, assume that the security objectives of the environment are satisfied with an indication of the security critical data on which each threat depends.

<i>Threat/ Objective</i>	<i>T1</i>	<i>T2</i>	<i>T3</i>	<i>T4</i>	<i>T5</i>	<i>T6</i>	<i>T7</i>
<i>O1</i>	✓						
<i>O2</i>	✓						
<i>O3</i>		✓					
<i>O4</i>	✓		✓	✓	✓	✓	✓
<i>O5</i>			✓	✓	✓		
<i>O6</i>					✓		
<i>O7</i>	✓		✓	✓	✓	✓	✓
<i>O8</i>	✓		✓	✓	✓	✓	✓
<i>O9</i>							✓
<i>O10</i>							✓

Table 6: Security Threat/Objective Cross-Reference

4.3.1.1 Countering the Confidentiality Threat

High information can only either directly (overtly) or indirectly (covertly) flow to the Low LAN Interface. O1 and O2, respectively, address these two possibilities. Since covert channels cannot practically be eliminated [6], we accept sufficient constraints on their existence as defined by the administrator in the NP configuration. Since these constraints are configurable, confidentiality also depends on providing administrative functions to properly maintain the configuration (O7) and constraints on those who may access those functions (O8). O4 ensures that users trying to access administrator functions are properly identified and authenticated.

4.3.1.2 Countering the Integrity Threat

The integrity of information stored on the High LAN depends (in part) on the NP's accurate transfer of information received from authorized Low LAN users. Objective O3 directly and completely addresses threat T2. The NP prevents unauthorized use of NP connection services (T3) by identifying and authenticating users (O4) and by allowing the administrator to maintain (O7) and enforce (O5) the list of allowable connections. Of course, only authorized administrators may modify the configuration, as required by O8.

4.3.1.3 Countering the Availability Threat

T4 and T5 constitute the threats to the availability of Low information on the High LAN that are addressed by the NP. T4 and T5 require making sure that only authorized users (O5) who have been properly authenticated (O4) can use NP connection services. T5 requires that authorized users of an NP connection be treated fairly when partitioning the communication bandwidth among those users (O6). T4 and T5 require that only authorized administrators (O8) be given access to administrative functions (O7) to ensure authorization of only valid connections and fair partitioning of the NP's throughput among those connections.

4.3.1.4 Countering the Configuration Threat

Proper configuration of the NP is the responsibility of the administrator. To allow him to do this task effectively, we provide functions (O7) that enables only authenticated (O4) administrators (O8) to properly manage the NP configuration.

4.3.1.5 Countering the Detection Threat

The efficacy of security audit depends on being able to log the events that indicate a security problem (O7 and O9) and to accurately identify (O4) the users responsible for malicious activity (O10) given an adequate review of the security audit logs. Review and management of audit logs are the responsibility of the administrator (OE1). O8 ensures that only authorized personnel can modify those logs.

Chapter 5 Security Requirements

This chapter describes the NP's security functional requirements in Section 5.1, the rational for these requirements in Section 5.2, and the NP's security assurance requirements in Section 5.3.

5.1 Security Functional Requirements (SFR)

The Common Criteria requires that NP's Security Functional Requirements (SFRs) be chosen from the set specified in [10]. That document categorizes the SFRs hierarchically. At the top of the hierarchy are SFR classes, which refine into SFR families. SFR families, in turn, refine into SFR components and finally into the SFRs themselves.

Table 7 details the security functional classes and components that constitute the NP SFR specification. Requirements in the Security Audit class involve recognizing, recording, storing and reviewing information related to security relevant activities. User Data Protection specifies requirements for NP confidentiality, integrity, and administrative functions and policies. Identification and Authentication specifies requirements that the identity of NP client users and administrators be established and verified. Security Management involves managing configuration and control functions and data, and limiting their access to authorized administrators. The Protection of TOE Security Functions class includes requirements that relate to the integrity and management of mechanisms that support or implement security functions. Resource Utilization specifies requirements that support the availability of required resources such as processing capability and/or storage capacity. The last two classes, TOE Access and Trusted Path/Channels, include requirements for restricting access to NP connections and for a trusted communication path from the Administrator Terminal, respectively.

<i>Functional Class</i>	<i>Functional Component</i>
Security Audit	FAU_GEN.1 Audit Data Generation
	FAU_SAR.1 Audit Review
	FAU_STG.2 Guarantees of Audit Data Availability
User Data Protection	FDP_ACC.1 Subset Object Access Control
	FDP_ACF.1 Security Attribute Based Access Control
	FDP_ACF.3 Access Authorization and Denial
	FDP_DAU.1 Basic Data Authentication
	FDP_IFC.2 Complete Information Control
	FDP_IFF.2 Simple Security Attributes
	FDP_IFF.4 Partial Elimination of Illicit Information Flows
	FDP_IFF.6 Illicit Information Flow Monitoring
Identification and Authentication	FIA_UAU.2 User Authentication before any action
	FIA_UID.2 User Identification before any action
Security Management	FMT_MSA.1 Management of Security Attributes
	FMT_MSA.3 Static Attribute Initialization
	FMT_MTD.1 Management of TSF Data
	FMT_REV.1 Revocation
	FMT_SMR.1 Security Roles

<i>Functional Class</i>	<i>Functional Component</i>
Protection of the TOE Security Functions	<i>FPT_AMT.1</i> Abstract Machine Testing
	<i>FPT_FLS.1</i> Failure with Preservation of Secure State
	<i>FPT_RCV.3</i> Automated Recovery without Undue Loss
	<i>FPT_RCV.4</i> Function Recovery
	<i>FPT_RVM.1</i> Non-Bypassability of the TSP
	<i>FPT_SEP.1</i> TSF Domain Separation
	<i>FPT_STM.1</i> Time Stamps
	<i>FPT_TST.1</i> TSF Testing
Resource Utilization	<i>FRU_FLT.1</i> Degraded Fault Tolerance
	<i>FRU_RSA.2</i> Minimum and Maximum Quotas
TOE Access	<i>FTA_TSE.1</i> TOE Session Establishment
Trusted Path/Channels	<i>FTP_TRP.1</i> Trusted Path

Table 7: The NP's Security Functional Requirement Classification

5.1.1 Requirements for Security Audit (FAU)

5.1.1.1 FAU_GEN.1 – Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the *Audit Log Events*.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: type of event, the identity of the agent causing the event, time of the event, and the *success or failure* of the event.

5.1.1.2 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide *authorized administrators* with the capability to read the *Audit Log Events* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 FAU_STG.2 – Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall store generated audit records in a permanent audit trail.

FAU_STG.2.2 The TSF shall ensure that the last *n KB of audit data* will be maintained independent of *audit storage exhaustion*.

5.1.2 Requirements for Data Protection (FDP)

5.1.2.1 FDP_ACC.1 - Subset Object Access Control

FDP_ACC.1.1 The TSF shall enforce the Admin Access Policy for all users accessing Admin Operations.

5.1.2.2 FDP_ACF.1 - Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the Admin Access Policy to objects based on the role of the user accessing Admin Operations.

FDP_ACF.1.2 The TSF shall ensure that only users authorized for the Administrator role can access Admin Operations on Admin Objects and that all new connection requests immediately enforce any changes to the NP configuration that result from these operations.

5.1.2.3 FDP_ACF.3 – Access Authorization and Denial

FDP_ACF.3.1 The TSF shall ensure that the access control SF that enforces the Admin Access Policy shall explicitly authorize access to Admin Operations for users authorized for the Administrator role.

FDP_ACF.3.2 The TSF shall ensure that the access control SF that enforces the Admin Access Policy shall explicitly deny access to Admin Operations for users not authorized for the Administrator role.

5.1.2.4 FDP_DAU.1 – Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of Client Objects.

FDP_DAU.1.2 The TSF shall be able to verify evidence of the validity of the indicated information.

5.1.2.5 FDP_IFC.2 - Complete Information Control

FDP_IFC.2.1 The TSF shall enforce the Information Flow Security Policy for all users and all operations performed by those users.

FDP_IFC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by the Information Flow Security Policy.

5.1.2.6 FDP_IFF.2 Simple Security Attributes

FDP_IFF.2.1 The TSF shall enforce the Information Flow Security Policy to associate with users and data one of two security levels, Low and High.

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and a controlled object via a controlled operation if the Information Confidentiality Rules hold.

FDP_IFF.2.3 The TSF shall enforce the Information Integrity Rules.

5.1.2.7 FDP_IFF.4 Partial Elimination of Illicit Information Flows

FDP_IFF.4.1 The TSF shall enforce the Information Flow Security Policy to limit the capacity of covert storage and timing channels from High LAN Interface to the Low LAN Interface to [maximum capacity].

FDP_IFF.4.2 The TSF shall prevent covert flows of High information stored internal to the NP to the Low LAN Interface.

5.1.2.8 FDP_IFF.6 Illicit Information Flow Monitoring

FDP_IFF.6.1 The TSF shall enforce the Information Flow Security Policy to monitor the possible exploitation of covert storage and timing channels.

5.1.3 Requirements for Identification and Authentication (FIA)

5.1.3.1 FIA_UAU.2 – User Authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any TSF-mediated actions on behalf of that user.

5.1.3.2 FIA_UID.2 - User Identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any TSF-mediated actions on behalf of that user.

5.1.4 Requirements for Security Management (FMT)

5.1.4.1 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the Admin Access Policy to restrict to users authorized for the Administrator role the ability to modify the roles of users.

5.1.4.2 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the Admin Access Policy to provide restrictive default values for object security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the Administrator role to specify alternate initial values to override the default values when an object is created.

5.1.4.3 FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to read or modify the Admin Objects to users authorized for the Administrator role.

5.1.4.4 FMT_REV.1 - Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke role permissions associated with users within the TSC to users authorized for the Administrator role.

FMT_REV.1.2 The TSF shall enforce *revocation of a user's Administrator role on the next authentication of that user.*

5.1.4.5 FMT_SMR.1 - Security Roles

FMT_SMR.1.1 The TSF shall maintain the *Administrator role.*

FMT_SMR.1.2 The TSF shall be able to associate users with this role.

5.1.5 Requirements for Protection of the TOE Security Functions (FPT)

5.1.5.1 FPT_AMT.1 – Abstract Machine Testing

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up and at the request of the authorized administrator* to demonstrate the correct operation of the security functions provided by the abstract machine which underlies the TSF.

5.1.5.2 FPT_FLS.1 – Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when *the system, a connection or the power fails.*

5.1.5.3 FPT_RCV.3 – Automated Recovery without Undue Loss

FPT_RCV.3.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the NP to a secure state is provided.

FPT_RCV.3.2 The TSF shall provide the authorized administrator with the capability to restore the TSF data to a consistent and secure state.

FPT_RCV.3.3 For *system, connection, or power failure*, the TSF shall return the NP to a secure state using automated procedures.

FPT_RCV.3.4 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored with *no* loss of TSF data or objects within the TSC.

5.1.5.4 FPT_RCV.4 – Function Recovery

FPT_RCV.4.1 The TSF shall ensure that *upon recovery from a system, connection, or power failure, user data successfully received over a recoverable connection before the failure is successfully delivered to the High LAN Interface once the connection is re-established.*

5.1.5.5 FPT_RVM.1 – Non-Bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before assignment operation within the TSC is allowed to proceed.

5.1.5.6 FPT_SEP.1 – TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.7 FPT_STM.1 – Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.5.8 FPT_TST.1 – TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self *tests during initial start-up and at the request of the authorized administrator* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of the TSF data.

FPT_TST.1.3 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code.

5.1.6 Requirements for Resource Utilization (FRU)

5.1.6.1 FRU_FLT.1 – Degraded Fault Tolerance

FRU_FLT.1.1 When *a particular connection fails*, the TSF shall ensure the continued operation of *all other NP connections*.

5.1.6.2 FRU_RSA.2 – Minimum and Maximum Quotas

FRU_RSA.2.1 The TSF shall enforce quotas limiting the maximum quantity of *the currently allocated connection resources* that *individual users* can use *over a specified period of time*.

FRU_RSA.2.2 The TSF shall ensure the provision of minimum quantity of *the currently allocated connection resources* that *individual users* can use *over a specified period of time*.

5.1.7 Requirements for TOE Access (FTA)

5.1.7.1 FTA_TSE.1 – TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session (connection) establishment based on *a user's location and/or port of access*.

5.1.8 Requirements for Trusted Path/Channels (FTP)

5.1.8.1 FTP_TRP.1 – Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path, the Administrator Interface between itself and *local* human users that is logically distinct from other communication paths and provides assured identification of its endpoints and the protection of the channel data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit *local users* to initiate communication via the Administrator Interface.

FTP_TRP.1.3 The TSF shall require the use of the Administrator Interface for *initial user authentication (as an authorized administrator) and to invoke the Admin Operations*.

5.1.9 Minimum Strength of Function Levels

The CC requires that the PP include a statement of the minimum strength of function level for the SFRs that are realized by a probabilistic or permutational mechanism (e.g., a password or hash function). The strength of function refers to “a qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanism”. The strength of function level is one of SoF-Basic, SoF-Medium, or SoF-High.

The mechanisms implementing the confidentiality requirements must meet a SoF-High strength of function level. This particularly applies to the constraints on the potential (illicit) leakage of High information to Low as captured in the FDP_IFF.4 requirements. The constraints on the covert channel capacities provides a strength of function metric that will be used to determine the acceptability of the functions enforcing confidentiality.

All other security mechanisms must be built to meet a SoF-Medium strength of function level.

5.2 Security Functional Requirements Rationale

Table 8 below cross-references the NP security objectives, identified in Section 4.1, against the security functional requirements, identified above. All of the security objectives depend intrinsically on the correctness of the underlying abstract base machine (FPT_AMT.1), the correctness of the security function (FPT_TST.1), the non-bypassability (FPT_RVM.1) and tamper resistance (FPT_SEP.1) of the security function, and the preservation of security upon failure (FPT_FLS.1) and upon recovery from failure (FPT_RCV.3). We therefore assume these dependencies, which are indicated in Table 8, in the following arguments that the SFR's are sufficient to satisfy the security objectives.

<i>SFR\OBJ</i>	<i>O1</i>	<i>O2</i>	<i>O3</i>	<i>O4</i>	<i>O5</i>	<i>O6</i>	<i>O7</i>	<i>O8</i>	<i>O9</i>	<i>O10</i>
<i>FAU_GEN.1</i>									✓	✓
<i>FAU_SAR.1</i>									✓	
<i>FAU_STG.2</i>									✓	
<i>FDP_ACC.1</i>								✓		
<i>FDP_ACF.1</i>					✓			✓		
<i>FDP_ACF.3</i>							✓	✓		
<i>FDP_DAU.1</i>					✓					
<i>FDP_IFC.2</i>	✓	✓	✓							
<i>FDP_IFF.2</i>	✓		✓							
<i>FDP_IFF.4</i>		✓								
<i>FDP_IFF.6</i>									✓	
<i>FIA_UAU.2</i>				✓						
<i>FIA_UID.2</i>				✓						
<i>FMT_MSA.1</i>								✓		
<i>FMT_MSA.3</i>								✓		
<i>FMT_MTD.1</i>								✓		

<i>SFR_OBJ</i>	<i>O1</i>	<i>O2</i>	<i>O3</i>	<i>O4</i>	<i>O5</i>	<i>O6</i>	<i>O7</i>	<i>O8</i>	<i>O9</i>	<i>O10</i>
<i>FMT_REV.1</i>								✓		
<i>FMT_SMR.1</i>							✓			
<i>FPT_AMT.1</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>FPT_FLS.1</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>FPT_RCV.3</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>FPT_RCV.4</i>			✓			✓				
<i>FPT_RVM.1</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>FPT_SEP.1</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>FPT_STM.1</i>									✓	
<i>FPT_TST.1</i>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
<i>FRU_FLT.1</i>						✓				
<i>FRU_RSA.2</i>						✓				
<i>FTA_TSE.1</i>					✓					
<i>FTP_TRP.1</i>								✓		

Table 8: Security Objective/Functional Requirement Cross-Reference

5.2.1 Satisfaction of Objective O1

FDP_IFC.2 ensures that the NP will enforce *Information Flow Security Policy* for all operations performed by all users, while FDP_IFF.2 ensures, through the *Information Confidentiality Rules*, that data classified High may be exported only to High users. This prohibits sending High data over the Low LAN Interface since Low users have access to it.

5.2.2 Satisfaction of Objective O2

Covert channels of High information can be split into those that flow from a High user/process over the High LAN Interface to the Low LAN Interface and those that flow from the NP itself to the Low LAN Interface. FDP_IFF.4 ensures the constraint of the former and the prevention of the latter. Mechanisms constraining the covert channels must meet a *SoF-High* strength of function level. FDP_IFC.2 ensures that these requirements will be enforced over all operations performed by all users.

5.2.3 Satisfaction of Objective O3

FDP_IFC.2 ensures that the NP will enforce *Information Flow Security Policy* for all operations performed by all users, while FDP_IFF.2 ensures that the *Information Integrity Rules* are enforced. The sequence of messages successfully received over the Low LAN Interface by the NP includes those, and only those, messages that a Low user wishes to be available on the High LAN. The delay inherent in NP processing means that, at any point, some prefix of these messages should be successfully delivered over the High LAN Interface. In the case of a non-recoverable connection, messages not delivered before failure may not be delivered at all. Nevertheless, this ensures the accurate relay of Low messages to the High LAN. FDP_RCV.4 makes explicit that recovery from a failed (recoverable) connection requires relaying all messages that were successfully received, but not yet successfully transmitted, before the failure occurred.

5.2.4 Satisfaction of Objective O4

FIA_UID.2 and FIA_UAU.2 ensure that the NP identifies and authenticates all users before allowing their access to security relevant function, as required. The authentication mechanisms will likely have to meet an SoF-Medium strength of function level.

5.2.4.1 Satisfaction of Objective O5

The data authentication requirements of FDP_DAU.1 provide a means to guarantee that data received by the NP came from a particular user from a particular location. FTA_TSE.1 ensures the ability to deny access to NP connection services based on this information. Changes to the accessibility of these services (i.e., the configuration) are made via the Admin Operations; FDP_ACF.1 ensures that any such changes will be enforced in any subsequent connection request.

5.2.5 Satisfaction of Objective O6

Authorized users of NP connection services must be given access to a connection whenever possible. If a particular connection fails, FRU_FLT.1.1 ensures that all other connections will continue service. Under more serious power or system failures, FRU_RCV.3 ensures that the NP will automatically recover to a secure state, where it can continue service by first delivering any messages not previously delivered successfully (FPT_RCV.4.1). Furthermore, by properly limiting the maximum quantity of connection resources consumable by a particular user over time (FRU_RSA.2.1) and ensuring the availability of some minimal set of resources (PRU_RSA.2.2), the NP ensures full and fair access to NP connection services.

5.2.6 Satisfaction of Objective O7

FMT_SMR.1 ensures that an Administrator role can be associated with NP users. FDP_ACF.3 ensures that the NP has function that permits authorized administrators to invoke the Admin Operations. No other functions are needed to effectively manage the NP configuration.

5.2.7 Satisfaction of Objective O8

The NP requirements to enforce the Admin Access Policy (FDP_ACC.1 and FDP_ACF.1.3) ensure that only users authorized for Administrator role can access Admin Operations; all other users are explicitly denied access. The Admin Operations constitute all of the security relevant administrative functions. FMT_MSA.3 and FMT_MTD.1 further spell out that no access to Admin Objects is permitted unless the user has Administrator role.

FMT_MSA.1 and FMT_REV.1 restricts modifying user roles to authorized administrators. Administrators are trusted to give such privileges only to trustworthy and competent personnel (see OE1). FMT_REV.1 also ensures that role privileges are up-to-date by requiring that any revocation of privilege take effect on that user's next authentication. Finally, FTP_TRP.1 ensures that the Admin Operations transmitted over the Administrator Interface are protected from interception or modification. Note that satisfying objective O8 assumes that the NP properly identifies and authenticates users, which O4 guarantees.

5.2.8 Satisfaction of Objective O9

The recording of the Audit Log Events required in FAU_GEN.1 and the monitoring of covert information flows in FDP_IFF.6 are sufficient to detect attacks to leak High information to the Low LAN Interface. Times stamps provided for in FPT_STM.1 may be particularly useful for identifying exploitation of existing covert timing channels. FAU_GEN.1 also records information vital to detecting malicious tampering with NP security administration function or data. FAU_STG.1 and FAU_SAR.1 ensure that the log information is maintained long enough and in a suitable format for analysis by an authorized administrator.

5.2.9 Satisfaction of Objective O10

FAU_GEN.1 requires audit log recording of the identity of the user that initiated the audit log event. This permits holding users accountable for their security relevant actions. . Note that satisfying objective O10 assumes that the NP properly identifies and authenticates users, which O4 guarantees.

5.2.10 Strength of Function Requirement Consistency

The NP is exclusively responsible for protecting the confidentiality of High information available over the High LAN Interface from leaking (overtly or covertly) to the Low LAN. As such, an SoF-High strength of function is mandated to ensure negligible leakage. This is supported by the covert channel constraints of FDP_IFF.4 and is consistent with the security objectives, in particular O1 and O2.

A lesser strength of function level, SoF-Medium, is required of the other security function. This is justified since confidentiality is the primary threat to linking Low and High enclaves. Without such a link, integrity and availability are subject to the limitation of manual methods for data transfer to move Low information to High. In addition, the NP plays a much less significant role in enforcing the integrity and availability requirements on which the NP's security functions are based. This is seen by the significant threats to integrity and availability that must be addressed by the NP's environment (see Section 3.2), if these threats are important to that environment.

5.2.11 Security Requirements Mutually Supportive

Table 9 below shows the functional dependencies among the SFRs, as defined by [10]. The table verifies that each dependency is met by one of the SFRs included or, in the case of an assurance requirement dependency, that EAL5 satisfies the dependency. The Letter H after a reference number indicates that a dependency is satisfied by a component that is hierarchical to the component required.

<i>Line #</i>	<i>SFR</i>	<i>Dependencies</i>	<i>Reference Line</i>
<i>1.</i>	FAU_GEN.1	FPT_STM.1	25
<i>2.</i>	FAU_SAR.1	FAU_GEN.1	1
<i>3.</i>	FAU_STG.2	FAU_GEN.1 FAU_SAR.1	1 2
<i>4.</i>	FDP_ACC.1	FDP_ACF.1	5
<i>5.</i>	FDP_ACF.1	FDP_ACC.1	4
<i>6.</i>	FDP_ACF.3	FDP_ACC.1	4
<i>7.</i>	FDP_DAU.1	--	
<i>8.</i>	FDP_IFC.2	FDP_IFF.1	9 (H)
<i>9.</i>	FDP_IFF.2	FDP_IFC.1	8 (H)
<i>10.</i>	FDP_IFF.4	AVA_CCA.1 FDP_IFC.1	EAL5 8 (H)
<i>11.</i>	FDP_IFF.6	AVA_CCA.1 FDP_IFC.1	EAL5 8 (H)
<i>12.</i>	FIA_UAU.2	FIA_UID.1	13 (H)
<i>13.</i>	FIA_UID.2	--	
<i>14.</i>	FMT_MSA.1	FDP_ACC.1 FDP_IFF.1	4 8 (H)

<i>Line #</i>	<i>SFR</i>	<i>Dependencies</i>	<i>Reference Line</i>
		FMT_SMR.1	18
15.	FMT_MSA.3	ADV_SPM.1 FMT_MSA.1 FMT_SMR.1	EAL5 14 18
16.	FMT_MTD.1	FMT_SMR.1	18
17.	FMT_REV.1	FMT_SMR.1	18
18.	FMT_SMR.1	FIA_UID.1	13 (H)
19.	FPT_AMT.1	--	
20.	FPT_FLS.1	ADV_SPM.1	EAL5
21.	FPT_RCV.3	ADV_SPM.1 AGD_ADM.1 FMT_SMR.1 FPT_TST.1	EAL5 EAL5 18 26
22.	FPT_RCV.4	ADV_SPM.1	EAL5
23.	FPT_RVM.1	--	
24.	FPT_SEP.1	--	
25.	FPT_STM.1	--	
26.	FPT_TST.1	FPT_AMT.1	19
27.	FRU_FLT.1	FPT_FLS.1	22
28.	FRU_RSA.2	--	
29.	FTA_TSE.1	--	
30.	FTP_TRP.1	--	

Table 9: Dependency Analysis

The analysis of dependencies among SFRs shows how some security requirements support other security requirements. For example, requirements for the review of audit log (FAU_SAR.1) depends on generating the audit data in the first place (FAU_GEN.1); thus, FAU_GEN.1 supports FAU_SAR.1. By definition, assurance requirements support the SFRs, since they provide confidence that the functional requirements are met. Therefore, the assurance requirements are mutually supportive since all of the dependencies are satisfied for the EAL5 level of assurance.

Table 10 shows how the SFRs mutually support each other beyond the dependencies described above. One SFR, call it SFR1, supports another SFR, SFR2, if

- SFR1 helps to prevent the bypass of SFR2,
- SFR1 helps to prevent tampering with the enforcement of SFR2 (including the tampering with any security critical data on which that SFR depends),
- SFR1 helps detect the (possible) violation of SFR2, or
- SFR1 helps recover from failures in a way that satisfies SFR2.

Table 10 lists the supporting SFRs for each SFR in each of these categories.

<i>SFR</i>	<i>Non-Bypassable</i>	<i>Tamperproof</i>	<i>Detection</i>	<i>Recovery</i>
<i>FAU_GEN.1</i> <i>FAU_SAR.1</i> <i>FAU_STG.2</i>	FPT_RVM.1	FPT_SEP.1 FDP_ACC.1 FDP_ACF.1 FDP_ACF.3	N/A	FPT_FLS.1 FPT_RCV.3
<i>FDP_ACC.1</i> <i>FDP_ACF.1</i> <i>FDP_ACF.3</i>	FPT_RVM.1 FIA_UAU.2 FMT_SMR.1	FPT_SEP.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_REV.1 FTP_TRP.1	FAU_GEN.1 FAU_SAR.1 FAU_STG.1	FPT_FLS.1 FPT_RCV.3
<i>FDP_DAU.1</i> <i>FTA_TSE.1</i> <i>FRU_FLT.1</i> <i>FRU_RSA.2</i>	FPT_RVM.1 FIA_UAU.2	FPT_SEP.1 FDP_ACC.1 FDP_ACF.1 FDP_ACF.3	FAU_GEN.1 FAU_SAR.1 FAU_STG.1	FPT_FLS.1 FPT_RCV.3
<i>FDP_IFC.2</i> <i>FDP_IFF.2</i>	FPT_RVM.1	FPT_SEP.1 FDP_ACC.1 FDP_ACF.1 FDP_ACF.3	FAU_GEN.1 FAU_SAR.1 FAU_STG.1	FPT_FLS.1 FPT_RCV.3 FPT_RCV.4
<i>FDP_IFF.4</i>	FPT_RVM.1	FPT_SEP.1 FDP_ACC.1 FDP_ACF.1 FDP_ACF.3	FAU_GEN.1 FAU_SAR.1 FAU_STG.1 FDP_IFF.6	FPT_FLS.1 FPT_RCV.3
<i>FDP_IFF.6</i> <i>FIA_UAU.2</i> <i>FIA_UID.2</i> <i>FMT_MSA.1</i> <i>FMT_MSA.3</i> <i>FMT_MTD.1</i> <i>FMT_REV.1</i> <i>FMT_SMR.1</i> <i>FPT_STM.1</i>	FPT_RVM.1	FPT_SEP.1 FTP_TRP.1	FAU_GEN.1 FAU_SAR.1 FAU_STG.1	FPT_FLS.1 FPT_RCV.3
<i>FPT_FLS.1</i> <i>FPT_RCV.3</i> <i>FPT_RCV.4</i>	Only invoked upon failure	FPT_SEP.1	N/A	N/A
<i>FPT_AMT.1</i> <i>FPT_TST.1</i>	Only invoked by administrator	FPT_SEP.1	N/A	N/A
<i>FPT_RVM.1</i>	By definition	FPT_SEP.1	N/A	N/A
<i>FPT_SEP.1</i>	FPT_RVM.1	By definition	N/A	N/A
<i>FTP_TRP.1</i>	By definition	FPT_SEP.1	N/A	N/A

Table 10: SFR Mutual Support

Bypass of the SFRs is primarily prevented by FPT_RVM.1, which requires that security enforcement functions always be invoked. The user authentication requirement, FIA_UAU.2 also prevents bypassing those the SFRs that enforce access control on administrative functions or NP connection services. Some SFRs are not supposed to be always invoked and thus are not relevant to the non-bypassability criterion.

Tampering with the security function is primarily prevented by FPT_SEP.1, which requires the separation of security domains. Restrictions on access to the administrative function and data, FDP_ACC and FDP_ACF prevent tampering with security relevant configuration parameters. Many of the Security Management requirements, in turn, prevent tampering with the administrative permissions. The trusted path to the administrator terminal also prevents tampering by users masquerading as administrator.

The audit requirements (FAU) support the detection of possible security violations involving the user/administrator data and function.

The fail secure (FPT_FLS.1) and recovery (FPT_RCV.3) requirements support the recovery of the user/administrator data and function upon system, connection or power failure.

5.3 NP Security Assurance Requirements

The Common Criteria requires that NP's Security Assurance Requirements (SARs) be chosen from the set specified in [12]. That document describes seven increasingly rigorous Evaluation Assurance Levels, EAL1 to EAL7, where a particular level of assurance contain a subset of the SARs contained at the next higher level. Each EAL contains SAR classes, which refine into SAR families. SAR families, in turn, refine into SAR components and finally into the SARs themselves.

Table 7 details the security assurance classes and components that constitute the NP SAR specification, at EAL5. The use of the NP to separate different mandatory security levels makes EAL5 the lowest level acceptable for NP implementation. Less rigorous development processes would not provide the confidence needed that High information does not flow to the Low LAN. The relative simplicity of the NP makes it a candidate for even higher levels, but development time constraints made this impossible on the first pass. We are attempting to meet the higher EAL requirements for configuration management and life cycle support, which should make moving to higher levels possible, if customer demand warrants it.

<i>Assurance Class</i>	<i>Assurance Component</i>
Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.3 Development tools CM coverage
Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Development	ADV_FSP.3 Semiformal functional specification
	ADV_HLD.3 Semiformal high-level design
	ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Modularity
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.2 Semiformal correspondence demonstration
	ADV_SPM.3 Formal TOE security policy model
Guidance documents	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance

<i>Assurance Class</i>	<i>Assurance Component</i>
Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_LCD.2 Standardized life-cycle model
	ALC_TAT.2 Compliance with implementation standards
Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing – low level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment	AVA_CCA.1 Covert channel analysis
	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.3 Relatively resistant

Table 11: Assurance Requirement Components for EAL5

The following presents verbatim the CC requirements for EAL5.

5.3.1 Requirements for Configuration Management (ACM)

The Configuration Management (CM) class contains three families: CM automation (ACM_AUT), CM capabilities (ACM_CAP), and CM scope (ACM_SCP). CM is an aspect of establishing that the functional requirements and specifications are realized in the implementation of the NP. CM meets these objectives by requiring discipline and control in the processes of refinement and modification of the NP. CM systems are put in place to ensure the integrity of the configuration items that they control, by providing a method of tracking these configuration items, and by ensuring that only authorized users are capable of changing them.

Developer action elements:

ACM_AUT.1.1D The developer shall provide a CM plan.

ACM_CAP.3.1D The developer shall use a CM system.

ACM_CAP.3.2D The developer shall provide CM documentation.

ACM_SCP.3.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.2C The CM plan shall describe how the automated tools are used in the CM system.

ACM_AUT.1.3C The CM system shall provide an automated means to ensure that only authorized changes are made to the NP implementation representation.

ACM_AUT.1.4C The CM system shall provide an automated means to support the generation of any supported TSF from its implementation representation.

ACM_AUT.1.5C The CM system shall provide an automated means to support the comparison of any two supported TSF versions, to ascertain the changes.

ACM_CAP.3.1C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.3.2C The configuration list shall describe the configuration items that comprise the NP.

ACM_CAP.3.3C The CM documentation shall describe the method used to uniquely identify the NP configuration items.

ACM_CAP.3.4C The CM plan shall describe how the CM system is used.

ACM_CAP.3.5C The CM documentation shall provide evidence that the CM system is working properly.

ACM_CAP.3.6C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.7C The CM system shall ensure that only authorized changes are made to the NP configuration items.

ACM_CAP.3.8C The CM system shall support the generation of all supported versions of the NP.

ACM_CAP.3.9C The acceptance plan shall describe the procedures used to accept modified or newly created TSF configuration items as part of the NP.

ACM_SCP.3.1C As a minimum, the following shall be tracked by the CM system: the NP implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, security flaws, and development tools and related information.

ACM_SCP.3.2C The CM documentation shall describe how configuration items are tracked by the CM system.

5.3.2 Requirements for Delivery and Operation (ADO)

Delivery and operation provides requirements for correct delivery, installation, generation, and start-up of the NP.

Developer action elements:

ADO_IGS.1.ID The developer shall document procedures to be used for the secure installation, generation, and start-up of the NP.

Content and presentation of evidence elements:

ADO_IGS.1.IC The documentation shall describe the steps necessary for secure installation, generation, and start-up of the NP.

5.3.3 Requirements for Development (ADV)

The development class encompasses four families of requirements for representing the TSF at various levels of abstraction from the functional interface to the implementation: functional specification (ADV_FSP), high-level design (ADV_HLD), implementation representation (ADV_IMP), and low level design (ADV_LLD). The development class also includes a family of requirements called representation correspondence (ADV_RCR) for a correspondence mapping between the various TSF representations, ultimately requiring a demonstration of correspondence from the least abstract representation through all intervening representations to the NP summary specification provided in the ST. The other family in the development class, TSF internals (ADV_INT), describes requirements for the internal structure of the TSF.

The paradigm evident for these families is one of a functional specification of the TSF, decomposing the TSF into subsystems, decomposing the subsystems into modules, showing the implementation of the modules, and demonstration of correspondence between all decompositions that are provided as evidence. The requirements for the various TSF representations are separated into different families, however, since some of the representations are not necessary for low assurance evaluations.

Developer action elements:

ADV_FSP.4.1D The developer shall provide a functional specification.

ADV_FSP.4.2D The developer shall provide a TSP.

ADV_FSP.4.3D The developer shall provide a formal TSP model.

ADV_FSP.4.4D The developer shall provide a demonstration of correspondence between the formal TSP model and the functional specification.

ADV_HLD.3.1D The developer shall provide the high-level design of the TSF.

ADV_IMP.2.1D The developer shall provide the implementation representations for the entire TSF.

ADV_INT.1.1D The developer shall design the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.

ADV_INT.1.2D The developer shall provide an architectural description.

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_RCR.2.1D The developer shall provide evidence that the least abstract TSF representation provided is an accurate, consistent, and complete instantiation of the functional requirements expressed in the ST.

Content and presentation of evidence elements:

ADV_FSP.4.1C The functional specification shall describe the TSF using both an informal and semiformal style.

ADV_FSP.4.2C The functional specification shall include both an informal and semiformal presentation of syntax, effects, exceptions, error messages, and semantics of all external TSF interfaces.

ADV_FSP.4.3C The functional specification shall include evidence that demonstrates that the TSF is completely represented.

ADV_FSP.4.4C The demonstration of correspondence between the formal TSP model and the functional specification shall describe how the functional specification satisfies the formal TSP model.

ADV_FSP.4.5C The demonstration of correspondence between the formal TSP model and the functional specification shall show that there are no security functions in the functional specification that conflict with the formal TSP model.

ADV_FSP.4.6C The formal TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_FSP.4.7C The formal TSP model shall include a rationale that demonstrates that policies of the TSP that are modeled are satisfied by the formal TSP model.

ADV_FSP.4.8C The formal TSP model shall justify that all policies of the TSP that can be modeled are represented in the formal TSP model.

ADV_HLD.3.1C The presentation of the high-level design shall be semiformal.

ADV_HLD.3.2C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.3.3C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.3.4C The high-level design shall identify the interfaces of the subsystems of the TSF.

ADV_HLD.3.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.3.6C The high-level design shall describe the separation of the TSF into TSP enforcing and other subsystems.

ADV_IMP.2.1C The implementation representations shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representations shall describe the relationships between all portions of the implementation.

ADV_INT.1.1C The architectural description shall identify the modules of the TSF.

ADV_INT.1.2C The architectural description shall describe the purpose, interface, parameters, and effects of each module in the TSF.

ADV_INT.1.3C The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.3C The low-level design shall describe the purpose of each module.

ADV_LLD.1.4C The low-level design shall define the interrelationships between the modules in terms of provided functionality and dependencies on other modules.

ADV_LLD.1.5C The low-level design shall describe the implementation of all TSP enforcing functions.

ADV_LLD.1.6C The low-level design shall describe the interfaces of each module in terms of their syntax and semantics.

ADV_LLD.1.7C The low-level design shall provide a demonstration that the TSF is completely represented.

ADV_LLD.1.8C The low-level design shall identify the interfaces of the modules of the TSF visible at the external interface of the TSF.

ADV_RCR.2.1C For each adjacent pair of TSF representations, the evidence shall demonstrate that all parts of the more abstract representation are refined in the less abstract representation.

ADV_RCR.2.2C For each adjacent pair of TSF representations, where portions of both representations are at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

ADV_RCR.2.3C For each adjacent pair of TSF representations, where portions of either representation are informally specified the demonstration of correspondence between those portions of the representations may be informal.

5.3.4 Requirements for Guidance documents (AGD)

The class "Guidance Documents" encompasses two families: administrator guidance (AGD_ADM) and user guidance (AGD_USR). The guidance documents class provides the requirements for user and administrator guidance documentation. For the secure installation and use of the NP it is necessary to describe all relevant aspects for the secure application of the NP.

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe how to administer the NP in a secure manner.

AGD_ADM.1.2C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.3C The administrator guidance shall contain guidelines on the consistent and effective use of the security functions within the TSF.

AGD_ADM.1.4C The administrator guidance shall describe the difference between two types of functions: those which allow an administrator to control security parameters, and those which allow the administrator to obtain information only.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the administrator's control.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall contain guidelines on how the security functions interact.

AGD_ADM.1.8C The administrator guidance shall contain instructions regarding how to configure the NP.

AGD_ADM.1.9C The administrator guidance shall describe all configuration options that may be used during secure installation of the NP.

AGD_ADM.1.10C The administrator guidance shall describe details, sufficient for use, of procedures relevant to the administration of security.

AGD_ADM.1.11C The administrator guidance shall be consistent with all other documents supplied for evaluation.

AGD_USR.1.1C The user guidance shall describe the TSF and interfaces available to the user.

AGD_USR.1.2C The user guidance shall contain guidelines on the use of security functions provided by the NP.

AGD_USR.1.3C The user guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall describe the interaction between user-visible security functions.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation delivered for evaluation.

5.3.5 Requirements for Life Cycle Support (ALC)

The class "Life Cycle Support" encompasses two families: development security (ALC_DVS) and life cycle definition (ALC_LCD). Life-cycle support is an aspect of establishing discipline and control in the processes of refinement of the NP during development and maintenance. Confidence in the correspondence between the NP security requirements and the NP is greater if security analysis and the production of the evidence are done on a regular basis as an integral part of the development and maintenance activities.

Developer action elements:

ALC_DVS.1.ID The developer shall produce development security documentation.

ALC_LCD.2.ID The developer shall establish a life-cycle model to be used in the development and maintenance of the NP.

ALC_LCD.2.2D The developer shall produce life-cycle definition documentation.

ALC_LCD.2.3D The developer shall use a standardized life-cycle model to develop and maintain the NP.

ALC_TAT.2.ID The developer shall identify the development tools being used for the NP.

ALC_TAT.2.2D The developer shall document the selected implementation dependent options of the development tools.

ALC_TAT.2.3D The developer shall describe the implementation standards to be applied.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe the physical, procedural, personnel, and other security measures that are used to protect the confidentiality and integrity of the NP during its development.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the NP.

ALC_LCD.2.1C The life-cycle definition documentation shall describe the model used to develop and maintain the NP.

ALC_LCD.2.2C The life-cycle definition documentation shall explain why the model was chosen and how it is used to develop and maintain the NP.

ALC_LCD.2.3C The life-cycle definition documentation shall demonstrate compliance with the standardized life-cycle model.

ALC_TAT.2.1C Any development tools used for implementation shall be well-defined.

ALC_TAT.2.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

5.3.6 Requirements for Tests (ATE)

The class "Tests" encompasses four families: coverage (ATE_COV), depth (ATE_DPT), independent testing (e.g., functional testing performed by evaluators) (ATE_IND), and functional tests (ATE_FUN). Testing establishes that the TSF exhibits the properties necessary to satisfy the functional requirements of the PP/ ST. Testing provides assurance that the TSF satisfies at least the security functional requirements, although it cannot establish that the TSF does no more than what was specified. Testing may also be directed toward the internals of the TSF, such as the testing of subsystems and modules against their specifications.

The aspects of coverage and depth have been separated from functional tests for reasons of increased flexibility in applying the components of the families. However, the requirements in these three families are intended to be applied together.

The independent testing has dependencies on the other families to provide the necessary information to support the requirements, but is primarily concerned with independent evaluator actions.

This class does not address penetration testing, which is directed toward finding vulnerabilities that enable a user to violate the security policy. Penetration testing is addressed separately as an aspect of vulnerability assessment in the class AVA.

Developer action elements:

ATE_COV.2.ID The developer shall provide an analysis of the test coverage.

ATE_DPT.3.ID The developer shall provide the analysis of the depth of testing.

ATE_FUN.1.ID The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_IND.2.ID The developer shall provide the NP for testing.

Content and presentation of evidence elements:

ATE_COV.2.IC The analysis of the test coverage shall demonstrate that the tests identified in the test documentation cover the TSF.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate the correspondence between the security functions and the tests identified in the test documentation.

ATE_DPT.3.IC The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the NP operates in accordance with the functional specification, high level design, and low level design of the TSF.

ATE_FUN.1.IC The test documentation shall consist of test plans, test procedure descriptions, and test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function.

ATE_FUN.1.4C The test results in the test documentation shall show the expected results of each test.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each security function operates as specified.

ATE_IND.2.1C The NP shall be suitable for testing.

5.3.7 Requirements for Vulnerability Assessment (AVA)

The class "Vulnerability assessment" encompasses four families: covert channel analysis (AVA_CCA), misuse (AVA_MSU), strength of NP security functions (AVA_SOF) and vulnerability analysis (AVA_VLA). The class addresses the existence of exploitable covert channels, the misuse or incorrect configuration of the NP, the ability for all critical security mechanisms to withstand direct attack and the definition and assessment of penetration tests to exploit vulnerabilities introduced in the development or the operation of the NP.

Developer action elements:

AVA_CCA.1.1D The developer shall conduct a search for covert channels for each information flow control policy.

AVA_CCA.1.2D The developer shall provide covert channel analysis documentation.

AVA_MSU.2.1D The developer shall document an analysis of the guidance documentation for conflicting and incomplete guidance.

AVA_MSU.2.2D The developer shall ensure that the guidance documentation contains no misleading or unreasonable guidance.

AVA_SOF.1.1D The developer shall identify all NP security mechanisms for which a strength of NP security function analysis is appropriate.

AVA_SOF.1.2D The developer shall perform a strength of NP security function analysis for each identified mechanism.

AVA_VLA.3.1D The developer shall perform and document an analysis of the NP deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.3.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_CCA.1.1C The analysis documentation shall identify covert channels.

AVA_CCA.1.2C The analysis documentation shall describe the procedures used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.

AVA_CCA.1.3C The analysis documentation shall describe all assumptions made during the covert channel analysis.

AVA_CCA.1.4C The analysis documentation shall describe the method used for estimating channel capacity, which shall be based on worst case scenarios.

AVA_CCA.1.5C The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.

AVA_CCA.1.6C The analysis documentation shall provide evidence that the method used to identify covert channels is informal.

AVA_MSU.2.1C The analysis documentation shall provide a rationale that demonstrates that the guidance is not conflicting and is complete.

AVA_SOF.1.1C The strength of NP security function analysis shall determine the impact of the identified NP security mechanisms on the ability of the NP security functions to counter the threats.

AVA_SOF.1.2C The strength of NP security function analysis shall demonstrate that the identified strength of the security functions is consistent with the security objectives of the NP.

AVA_SOF.1.3C Each strength claim shall be either basic, medium, or high.

AVA_VLA.3.1C The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the NP.

AVA_VLA.3.2C The documentation shall justify that the NP, with the identified vulnerabilities, is relatively resistant to penetration attacks.

Chapter 6 Summary Specification

This chapter characterizes the functions that the NP uses to satisfy the security functional requirements described in the previous chapter. Sections 6.1 lists the security functions, respectively. Sections 6.2 traces these functions back to the requirements from which they derive.

6.1 Security Functions (SF)

The security functions described in this section are partitioned into those that promote confidentiality, integrity, identification and authentication, availability, provision of administrative function, administrative control, security audit, self test and secure failure and recovery. The security functions are stated in the form of requirements. These requirements form a subset of the overall “system” requirements being used to implement the NP. This approach ensures a clean mapping from this security target specification into the NP development.

The security functions described here assume that each NP connection be in one of three states - Connection Establishment, Connection Use, or Connection Termination - as shown in Figure 3. Connection Use is the only state in which data message traffic is being transmitted through the NP. The only activities in the Connection Establishment and Termination states are for setup and termination of an NP connection.

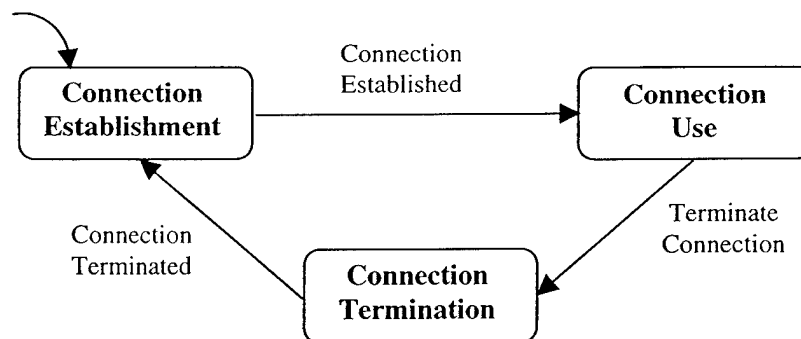


Figure 3: States of a NP Connection

The NP's operation requires the following additional assumption, which must hold in the environment in which it is embedded.

SFA1. If the authentication of messages is disabled, as defined by the Configuration Table, the NP environment will ensure the identity and authenticity of users accessing High and Low IP address/port number.

6.1.1 Functions for Confidentiality

The NP's approach to preserving the confidentiality of High information is to enforce a strict protocol, the Pump Protocol, for communication over the LAN Interfaces and to constrain the covert channels that this protocol permits. The NP limits the covert channels to a negligible capacity chosen by an authorized administrator. Domain separation prevents leakage of any High information stored internally.

SF1. The NP shall communicate over the High LAN Interface only via the Pump Protocol.

- SF2. The NP shall communicate over the Low LAN Interface only via the Pump Protocol.
- SF3. The NP shall discard any message received that is not in accordance with the Pump Protocol.
- SF4. During Connection Use, the only messages accepted by the NP over the High LAN Interface shall be acknowledgements that correspond to data messages transmitted from the NP to the High Wrapper.
- SF5. During Connection Use, the only messages sent by the NP over the Low LAN Interface shall be acknowledgments in a fixed, pre-specified format sent to the Low Wrapper.
- SF6. During Connection Use, the timing of acknowledgments from the NP to the Low Wrapper shall be controlled according to the algorithm provided in [1].
- SF7. During Connection Establishment and Termination, the number of Connection Request re-tries and the frequency of successful re-connections shall be constrained as defined by the current Configuration Table.
- SF8. The NP shall maintain a Low domain separate from the High Domain, with no access to High information, for executing all NP processes that communicate over the Low LAN Interface
- SF9. The NP shall maintain a High domain separate from the Low domain for executing all NP processes that communicate over the High LAN Interface.

6.1.2 Functions for Integrity

The NP's approach to ensure the integrity of Low information sent to High is to preserve the content and the sequential order of data messages received.

- SF10. Each data message delivered by the NP to the High Wrapper over the connection shall correspond exactly to a message successfully received from the Low Wrapper.
- SF11. The NP shall send data messages to the High Wrapper in the same order they are successfully received from the Low Wrapper.
- SF12. For each recoverable connection, the NP shall successfully deliver each data message successfully received from the Low Wrapper to the High Wrapper exactly once.
- SF13. For each non-recoverable connection, the NP shall successfully deliver each data message successfully received from the Low Wrapper to the High Wrapper at most once.

6.1.3 Functions for Identification and Authentication

NP users include administrators and connection clients. The NP identifies and authenticates administrators using a password mechanism accessible only via the Administrator Interface. Connection clients can be authenticated on a per message basis using a data authentication mechanism called MD5.

- SF14. The Administrator Interface of the NP shall comply with EIA RS-232.
- SF15. The NP shall be configured and controlled only via the Administrator Interface.
- SF16. The NP shall require password protection of the configuration and control functions that are available at the Administrator Interface.
- SF17. The NP shall require passwords to be at least eight characters long.

SF18. If the authentication of messages is enabled in the Configuration table, the NP shall authenticate all messages received over the Low LAN Interface and the High LAN Interface.

SF19. If the authentication of messages is enabled in the Configuration table, the NP shall use the MD5 Algorithm [7] to authenticate messages.

SF20. If the authentication of messages is enabled in the Configuration table, the NP shall discard all messages that do not pass the message authentication check.

6.1.4 Functions for Availability

The NP's approach to ensure the availability of Low information on the High LAN is to distribute connection resources fairly, to guarantee a minimum average throughput per connection, and to promote speedy and (if possible) automated recovery from failure with partial (degraded) connection operation where possible.

SF21. Each connection processed by the NP shall be independent of any other connection.

SF22. The NP shall use the max-min fairness policy [1] to allocate resources to individual connections.

SF23. The NP shall provide a connection establishment between the Low Wrapper and the High Wrapper on a first-come, first-serve basis.

SF24. The NP shall support a maximum number, greater than three, of simultaneous connections as defined by the Configuration Table.

SF25. For a particular connection, the NP shall be able to receive data from the Low Wrapper at the same rate that the High Wrapper accepts data from the NP.

SF26. The NP shall be capable of supporting combined throughput (of all active connections) of at least 2 megabits per second, from Low to High.

6.1.5 Functions for Administrative Provision

The administrator operations required by the SFRs are a subset of those provided by the SFs.

SF27. The NP shall provide the configuration and control capability at all times (on-line and off-line).

SF28. The NP shall support as configurable items the parameters of the Configuration Table.

SF29. The NP shall provide the capability to view the existing Configuration Table via the Administrator Interface.

SF30. The NP shall provide the capability to close a connection via the Administrator Interface.

SF31. The NP shall provide the capability to view the existing Status Log via the Administrator Interface.

SF32. The NP shall provide the capability to clear the Status Log via the Administrator Interface.

SF33. The NP shall provide the capability to view the existing Error Log via the Administrator Interface.

SF34. The NP shall provide the capability to clear the Error Log via the Administrator Interface.

SF35. The NP shall provide the capability to send Configuration Table, Status Log, and Error Log data to a Host on the High LAN.

SF36. The NP shall provide the capability to initiate, only via the Administrator Interface, transfer of the Configuration Table, Status Log and Error Log data to a specified Host on the High LAN.

SF37. The NP shall provide a Self-Test Command via the Administrator Interface, which shall execute the Built-In Test.

SF38. The NP shall report the results of the BIT to the System Operator via the Administrator Interface.

6.1.6 Functions for Administrative Control

The NP provides only one password-protected administrator account from which configuration and control functions and data can be accessed. The NP expedites the enforcement of any changes to the NP configuration, including the administrator account password.

SF39. The NP shall provide exactly one administrator account for accessing the configuration and control functions.

SF40. The NP shall ensure that only the authorized administrator can access the configuration and control functions that are available at the Administrator Interface.

SF41. The NP shall ensure that only the authorized administrator can access the configuration control data, which includes the Configuration Table and its parameters, the error log, the status log and administrator account password.

SF42. The NP shall immediately enforce changes to the Configuration Table for all new connection requests.

SF43. The NP shall provide the capability to initialize and modify the administrator's password via the Administrator Interface.

SF44. The NP shall enforce any changes the administrator's password on the next login.

6.1.7 Functions for Security Audit

The NP provides an audit log that is split into a status log, for successful operations, and an error log, for unsuccessful operations. These logs are guaranteed to hold at least n KB of the most recent audit data using a circular queue-style buffer.

SF45. The NP shall maintain a Status Log that records the following data:

- a the start and stop time of the current logging;
- b the type, agent and time of the event logged;
- c The number of connections initiated by the Low Wrapper since the Pump started;
- d The number of connections that are currently in the INUSE or ABORTED state;
- e The number of messages in the stable buffer for connections that are in the INUSE or ABORTED (total and per connection);
- f The total number of messages received and delivered for each connection tat is currently in the INUSE or ABORTED state;
- g The average time elapsed before the Pump sent a DMA to the Low Wrapper;
- h The total connection time (per connection) for each connection that is in the INUSE state;
- i The time each connection has been in the ABORTED state;
- j The current moving average values for each connection that is in the INUSE state. This represents the average time elapsed before the Pump received a DMA message from the High wrapper;

- k The number of connections terminated normally. This value is reset to zero each time the Pump starts;

SF46. The NP shall maintain a Error Log that records the following data:

- a the start and stop time of the current logging;
- b the type, agent and time of the event logged;
- c The number of erroneous messages received which are not in accordance with the Pump Protocol. This value is reset to zero each time the Pump starts.
- d The number of connections that terminated abnormally (terminated state is ABORTED) since the Pump started. This value is set to zero each time the NP starts.
- e The number of rejected connection requests. This value is reset to zero each time the NP starts.

SF47. The NP shall be able to hold at least x KB in the Status Log buffer.

SF48. In the event that the Status Log is full, the NP shall re-use the buffer in such a way that the oldest records are lost and the most recent records are retained.

SF49. The NP shall be able to hold at least $n-x$ KB records in the Error Log buffer.

SF50. In the event that the Error Log is full, the NP shall re-use the buffer in such a way that the oldest records are lost and the most recent records are retained.

6.1.8 Functions for Self-Test

NP self test includes a built-in test and checks on the integrity of both code and administrative data.

SF51. The NP shall check its internal operations through a built-in test (BIT).

SF52. The NP shall execute the BIT at power-up, at reset, and when commanded by the Administrator.

SF53. The NP shall provide authorized administrators with the capability to verify the integrity of configuration and control data.

SF54. The NP shall provide authorized administrators with the capability to verify the integrity of its stored executable code.

6.1.9 Functions for Secure Failure and Recovery

Functions for the NP's recovery from failure maintain the integrity of administrative data, shutdown communication when warranted, and ensure deliver of message not yet before the failure occurred.

SF55. Upon system, connection, or power failure, the NP shall maintain the integrity of the configuration data.

SF56. Upon system failure, the NP shall perform graceful shutdown and inhibit all communications over the Low LAN Interface and the High LAN Interface.

SF57. Upon connection failure with the Low Wrapper/Low Host, the NP shall deliver all messages in its queue to the High Wrapper.

SF58. Upon recovery from system, connection, or power failure, the NP shall deliver any messages that were successfully received over a recoverable connection and not successfully delivered before the failure occurred.

6.2 Security Function Rationale

Table 12 below cross-references the NP security functional requirement, identified in Section 5.1, against the security functions, identified in the previous section. The arguments that follow demonstrate that the combination of the security functions work together so as to satisfy the SFRs. The arguments are partitioned along the same lines as the SFs with two additional arguments for non-bypassability and domain separation.

[illegible]

[illegible]

Table 12: Security Functional Requirement/Security Function Cross-Reference

6.2.1 Confidentiality Argument

This argument completely satisfies FDP_IFF.4, and partially satisfies FDP_IFC.2, FDP_IFF.2.

The basis for information flow confidentiality is the *Information Flow Security Policy* (FDP_IFC.2), which includes restricting overt channels in the *Information Confidentiality Rules* of FDP_IFF.2 and restricting covert channels in FDP_IFF.4. Overt channels are prevented in SF1 and SF2 by requiring communication over the Low LAN Interface and the High LAN Interface only via the *Pump Protocol* [5], and in SF3 by

ignoring any messages not in accordance with this protocol. An analysis of the protocol shows that no overt channels are permitted.

Analysis of the *Pump Protocol* also shows that the only covert channels from the High LAN Interface to the Low LAN Interface are those that misuse the acknowledgment of data messages, during Connection Use, and those that misuse the connection negotiation process, during Connection Establishment and Termination. During Connection Use, SF4 and SF5 limit the form of covert channels possible by ensuring that only acknowledgements can be received from High and sent to Low, and that those sent to Low must be in a fixed, pre-specified format. The only covert channel that remains in this case is a timing channel exploitable through the modulation of the rate of acknowledgements by a High process, which is controlled in SF6. The algorithm cited constrains the covert channel as required by FDP_IFF.4. SF7 describes the constraints of the only covert channels from the High LAN Interface to the Low LAN Interface during Connection Establishment and Termination, i.e., channels exploited by allowing High to deny/approve connection requests by Low. These requirements also satisfy the covert channel constraints imposed by FDP_IFF.4. The FDP_IFF.4 constraints are sufficient to meet the *SoF-High* strength of function level. The strength of function analysis, given in section 6.2.13, describes the argument that these security functions constrain the covert channels as required by FDP_IFF.4.

The only other covert channels possible are from the NP itself to the Low LAN Interface which are exploitable only if the NP stores High information internally and only if malicious or erroneous function in the NP permits High information to leak. Although we do not prohibit storing High information altogether, SF8 and SF9 do prevent any NP processes that communicate over the Low LAN Interface from accessing High information and from interacting directly with processes that communicate over the High LAN Interface. Combined with the protection of administrative authentication data required by OE3 and configuration management constraints imposed by EAL5, which protect the NP from unauthorized modification, this makes it extremely difficult, if not impossible, to exploit this class of covert channels.

6.2.2 Integrity Argument

This argument completes the coverage of FDP_IFC.2 and FDP__IFF.2, when combined with the Confidentiality Argument.

The basis for information flow integrity is the *Information Flow Security Policy* (FDP_IFC.2), which includes the *Information Integrity Rules* of FDP_IFF.2. Thus, we must show that SF10 through SF12 ensure that the sequence of data messages successfully delivered by the NP over the High LAN Interface is a prefix (or subsequence for non-recoverable connections) of the sequence of data messages successfully received by the NP over the Low LAN Interface. Assumption A1 ensures that all data messages transmitted over the High LAN Interface go to the High Wrapper and, similarly, that all data messages received over the Low LAN Interface come from the Low Wrapper. For recoverable connections, each data message successfully received is successfully delivered exactly once (SF12), in the same order received (SF11), and with no spurious messages interspersed (SF10). This satisfies the prefix property required. For non-recoverable connections, each data message successfully received is successfully delivered at most once (SF13), in the same order received (SF11), and with no spurious messages interspersed (SF10). This satisfies the sub-sequence property required.

6.2.3 Identification and Authentication Argument

This argument completely satisfies FIA_UAU.2, FIA_UID.2 and FTP_TRP.1.

NP users include administrators, who access administration functions from the Administrator Interface and clients who use NP connection services from either the Low LAN Interface for the High LAN Interface. SF14, in combination with assumption A1, ensures the distinct communication path and assured endpoint identification that is required by FTP_TRP.1.1. SF15 and SF16 ensure that users at the Administrator Terminal must authenticate themselves over the Administrator Interface before using the interface to access *Admin Operations*, as required by FTP_TRP.1.2 and FTP_TRP.1.3. SF16 and SF16 ensure that, before being given access to administration functions, administrators are identified and authenticated using passwords that are at least 8 characters long. OE3 ensures that only authorized users are given the administrator

password and, once obtained, users protect their passwords from disclosure adequately. Therefore, SF16 and SF16 cover FIA_UAU.2 and FIA_UID.2 for all administrative actions.

The only other security relevant actions are those that involve use of the NP connection services by NP clients. 0 ensures that the environment identifies and authenticates users accessing High and Low IP address/port number, if the NP authentication of messages is disabled in the current configuration. If authentication of messages is enabled, SF18 and SF19 ensure that messages are authenticated using the MD5 algorithm. OE3 ensures that the MD5 private keys are distributed only to authorized client and that those clients protect them adequately. Before being permitted to use NP connection services, i.e., transmit messages over a connection, messages must pass the MD5 check, ensuring that the message is from an authorized client. SF20 guarantees that the NP discards any message that fails the MD5 check. Therefore, these security functions cover FIA_UAU.2 and FIA_UID.2 for all uses of an NP connection.

6.2.4 Connection Control Argument

This argument completely satisfies FDP_DAU.1 and FTA_TSE.1.

The Pump Protocol ensures that the NP can deny a request for use of NP connection services based on the source address/port number and destination address/port number. Therefore, SF1, SF2, and SF3 provide function that satisfies FTA_TSE.1. If the authentication of messages is enabled in the Configuration Table, the validity of Client Objects can be guaranteed by the authentication provided by the MD5 algorithm in SF18, SF19, and SF20, thus satisfying FDP_DAU.1. OE3 ensures that the MD5 private keys are distributed only to authorized client and that those clients protect them adequately. Before being permitted to use NP connection services, i.e., transmit messages over a connection, messages must pass the MD5 check, ensuring that the message is from an authorized client.

6.2.5 Availability Argument

This argument completely satisfies FRU_FLT.1 and FRU_RSA.2.

The NP is required to ensure that, once access to the NP connection services is granted, users get a fair share of the total communication bandwidth. FRU_RSA.2 does this by enforcing quotas on the maximum and minimum amount of connection resources allocated to the current NP connection users over time. Functions supporting fairness among users implement a max-min fairness policy for allocating the communication bandwidth (SF22) and a first-come, first-serve granting of connection requests (SF23). As described in [1], the max-min fairness policy allocates bandwidth to individual connections according to the following criterion – “the smallest realized rate is as large as possible and, given this, the second-smallest realized rate is as large as possible, etc.” They give the example that if three connections have demand rates .4, .5, and .6 messages per unit time, then each connection gets 1/3 of the bandwidth under max-min fairness.

Giving preferences to connections that have lower demand rate in this manner, prevents monopolizing resources by those connections that have higher demand rate, thus, enforcing the maximum quota required by FRU_RSA.2.1. It also ensures that the connections that have higher demand rates get at least as much resources as those with lower demand rates, thus enforcing the minimum quota required by FRU_RSA.2.2. Functions SF24 through SF26 ensure support for at least three connections with 2/N megabits per second minimum throughput per connection, where N is the maximum number of simultaneous connections permitted by the Configuration Table.

The requirement in FRU_FLT.1 that failure of one connection does not effect the operation of other connections is satisfied by the independence of individual connections given in SF21. The availability of NP connection services under other failures is managed by the automated recovery of the NP as described in the Secure Failure and Recovery argument.

6.2.6 Administrative Provision Argument

This argument partially satisfies FDP_ACF.3

The mapping of the administrative functions required in FDP_ACF.3, as indicated by the Admin Operations, to those provided by the SFs is straightforward. SF27 ensures that these operations are always available; the next section will argue that they are available only to authorized administrators. SF28 through SF38 provide functions for all of the Admin Operations. The audit log referred to in the Admin Operations is a combination of the status log and the error log provided by the SFs.

6.2.7 Administrative Control Argument

This argument completely satisfies FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, and FMT_SMR.1. This argument completes coverage of FDP_ACF.3 (when combined with the Administrative Provision Argument).

FDP_ACF.1.1 requires the NP to enforce the Admin Access Policy based on the role of a user, as supported in FMT_SMR.1. Roles are only implicitly supported in the SFs – any user with access to the Administrator Terminal and the administrator password is implicitly authorized for the Administrator role. This is acceptable since OE3 ensures that passwords are properly distributed and protected. Users without access to this password are denied access to Admin Operations, as required by FDP_ACF.3.2. SF15 ensures that users can access configuration and control functions only from the Administrator Interface. SF40 and SF41 ensure that only the authorized administrator can access configuration and control function and data, as required by FDP_ACF.1, FMT_MTD.1, and FMT_MSA.3.1. SF42 supports the immediate enforcement of changes to the configuration table required by FDP_ACF.1.2. Since the administration objects are not created dynamically, FMT_MSA.3.2 is irrelevant.

The SFs also simplify matters by requiring there to be exactly one administrator account in SF39. This eliminates the need to have a special super-user account to manage the accounts of different administrators. So there is one administrator account, the user of which can manage his own password according to SF43 and SF44, as required by FMT_MSA.1 and FMT_REV.1.

6.2.8 Security Audit Argument

This argument completely satisfies FAU_GEN.1, FAU_SAR.1, FAU_STG.2, FDP_IFF.6, and FPT_STM.1.

The SFs partition the NP audit log into a status log, which records information about operations that succeed and thus change the current status, and an error log, which records information about unsuccessful or erroneous operations. As defined in SF45 and SF46, the events recorded in each of these logs includes all of the Audit Log Events required by FAU_GEN.1.1 (except for the administrator operations) and monitors the potential covert channels as required by FDP_IFF.6. Administrator operations are not logged because there is only one administrator whose access requires authentication and, by OE1, he is trusted to perform his duties properly.

SF45 and SF46 also include the information required by FAU_GEN.1.2 (type, time stamp, and event agent (in the form of source/destination IP address and port number)). The inclusion of a time stamp in this report implicitly satisfies the requirement of FPT_STM.1.1. The capability to read the logs, required by FAU_SAR.1, is met by the administrator functions provided in SF31 and SF33. Finally, the functions SF47 through SF50 satisfy the requirements of FAU_STG.2.

6.2.9 Self-Test Argument

This argument completely satisfies FPT_AMT.1 and FPT_TST.1.

The built-in test functions of SF51 and SF52 implement the abstract machine test and the self test required by FPT_AMT.1.1 and FPT_TST.1.1. SF53 and SF54 provide the capability to check the validity of both the TSF data and code, as required by FPT_TST.1.2 and FPT_TST.1.3.

6.2.10 Secure Failure and Recovery Argument

This argument completely satisfies FPT_FLS.1, FPT_RCV.3, and FPT_RCV.4.

For the NP, a “secure state” refers to a state in which the configuration and control data are valid and the NP continues the correct enforcement of the Information Flow Security Policy and the Admin Access Policy. The types of failures that must be considered are system failure (which includes BIT failure), connection failure, and power failure. OE4 ensures that the NP storage media is protected from failure leading to loss or corruption of configuration and control data.

SF55 ensures the integrity of the configuration and control data upon failure, which includes authentication data used for ensuring that all administrators are authorized. SF56 ensures that, upon system failure, the NP will inhibit communications over the Low LAN Interface and the High LAN Interface. These functions ensure that the secure state required by FPT_FLS.1.1 and FPT_RCV.3.1 through FPT_RCV.3.3 is always maintained automatically. Finally, SF57, SF58, SF10, SF11, and SF12 ensure that failure of a recoverable connection causes no loss of messages successfully received over the Low LAN Interface and that, if not successfully delivered, these messages are sent as soon as possible. This, therefore, satisfies the requirements of FPT_RCV.3.4 and FPT_RCV.4.1.

6.2.11 Non-Bypassability Argument

This argument completely satisfies FPT_RVM.1.

The SFs that enforce the non-bypassability of the Information Flow Security Policy and the Admin Access Policy are functions for Confidentiality, Integrity, Identification and Authentication, Administrator Control, Self-Test and Secure Failure and Recovery. The preceding arguments made for each of these sets of functions ensure that the security mechanisms are invoked whenever needed to satisfy the security policies.

6.2.12 Domain Separation Argument

This argument completely satisfies FPT_SEP.1.

Because of the physical protection of the NP (OE2) and the restrictions permitting only authorized administrator access to configuration and control functions and data (SF40 and SF41), only trusted subjects can have direct contact with the NP. The only contact with untrusted subjects is via the Low LAN Interface and the High LAN Interface. This contact is restricted to sending and receiving messages. SF8 and SF9 support two domains that physically separate the processes that communicate over these interfaces.

6.2.13 Strength of Function Levels for Security Functions

The functions implementing the constraints on the covert channels due to the modulation of the timing of acknowledgments from the NP to the Low Wrapper (SF6) and to the manipulation of the Connection Request re-tries (SF7) must meet the SoF-High strength of function level. Since both of these covert channels are very difficult to exploit [1,3] and have capacities constrained as described in FDP_IFF.4 (*we need to describe why this is the case*), the correct implementation of SF6 and SF7 is sufficient to attain the SoF-High level.

The function implementing the password authentication of administrators (SF14) must meet a SoF-Medium strength of function level. The correct implementation of a password authentication scheme that requires passwords to be at least eight characters long (SF16) is sufficient to attain the SoF-Medium level.

The function implementing the authentication of data messages (SF18) must meet a SoF-Medium strength of function level. The MD5 algorithm [7] “takes as input a message of arbitrary length and produces a 128-bit ‘fingerprint’ or ‘message digest’ of the input. ... The MD5 algorithm is intended for digital signature applications, where a large file must be ‘compressed’ in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA”. The developers of the algorithm argue that “the difficulty of coming up with two messages having the same message digest is on the order of 2^{64} operations, and that the difficulty of coming up with any message having a

given message digest is on the order of 2^{128} operations.”[7] Therefore, the correct implementation of the MD5 algorithm is sufficient to attain the SoF-Medium level.

References

1. Kang, M.H., I.S. Moskowitz, D.C. Lee, "A Network Pump," *IEEE Transaction on Software Engineering*, Vol. 22, No. 5, May 1996.
2. Kang, M., and I. Moskowitz, "A Pump for Rapid, Reliable, Secure Communication," *Proc. 1st ACM Conf. on Computer and Communications Security*, Fairfax, VA, Nov. 1993, pp. 119-129.
3. Kang, M. H., A.P. Moore, and I.S. Moskowitz, "Design and Assurance Strategy for the NRL Pump," *Proc. Second IEEE Workshop on High Assurance Systems Engineering*, Aug. 1997, to appear.
4. Comer, D.E. *Internetworking with TCP/IP*, Vol. I, Second Ed., Prentice-Hall, 1991.
5. Naval Research Laboratory, "Network Pump Protocol," Technical Report NRL-PUMP-PRO-97-001, 16 Oct 1997.
6. Moskowitz, I.S. and M.H. Kang, "Covert Channels --- Here to Stay?," COMPASS '94, 1994.
7. Rivest, R., "The MD5 Message-Digest Algorithm," MIT Laboratory for Computer Science Technical Memorandum, April 1992.
8. Girling, C. Gray, "Covert Channels in LANs," *IEEE Transactions on Software Engineering*, Vol. SE-13 (2) Feb., 1987.
9. Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation; Part 1: Introduction and general model," Version 2.0, CCIB-97/081R, 19 December 1997.
10. Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation; Part 2: Security functional requirements," Version 2.0, CCIB-97/082R, 19 December 1997.
11. Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation; Part 2: Annexes," Version 2.0, CCIB-97/082AR, 19 December 1997.
12. Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation; Part 3: Security assurance requirements," Version 2.0, CCIB-97/083R, 19 December 1997.

Appendix A

Glossary

Admin Access Policy

Admin Objects

- 1 Configuration Table
- 2 Configuration Table parameters
- 3 Error log
- 4 Status log
- 5 Administrator authorization data
- 6 Administrator authentication data

Admin Operations

- 1 Instantiate the Configuration Table parameters
- 2 View the configuration table
- 3 Close a connection
- 4 View the existing audit log
- 5 Clear the audit log
- 6 Send the Configuration Table, status and error log data to the High LAN Interface.
- 7 Execute Self Test

Audit Log Events

- a) Start-up and shutdown of the audit functions;
- b) *Administrator operations;*
- c) *Communication with the High LAN Interface or the Low LAN Interface that deviates from established protocols;*
- d) *Periodic assessment of the timing of communications from the High LAN to the NP and from the NP to the Low LAN;*
- e) *Requests for connection;*
- f) *Termination of a connection.*

Client Objects

- 1 Data messages
- 2 Control messages

Configuration Table

This table shall contain the following information:

- Valid Low IP addresses and ports for transmitting requests and data to the NP
- Valid High IP addresses and ports for receiving data from the NP
- Valid connections (Low/High IP address/port pairs) [and whether recoverable connections are permitted for each pair]

- Enable/Disable authentication of all messages between the Low Wrapper and the NP for a valid connection
- Enable/Disable authentication of all messages between the NP and the High Wrapper for a valid connection
- Private key for message authentication between the Low Wrapper and the NP for a valid connection
- Private key for message authentication between the NP and the High Wrapper for a valid connection
- Window size (number of messages that Low Wrapper may transmit to Network Pump prior to receiving any acknowledgment) for each valid connection
- Number of intervals (time message delivered to High Wrapper, time acknowledgment received from High Wrapper) used to compute the moving average for a connection
- Maximum data message length
- Maximum number of simultaneous connections per Low host (IP address)
- Maximum number of simultaneous connections for the NP
- Fair size per connection [1]
- Network inactivity timeout value (maximum time the NP will wait to complete the transaction/reception of a Pump Protocol message)
- Status log size
- Error log size
- Abnormal re-connect frequency
- Maximum number (n) of connection request re-tries
- Time interval (t) between connection request re-tries
- Normal re-connect frequency
- Valid High IP address and port for receiving Configuration, Status, and Error Log data from the NP

Information Confidentiality Rules

Data classified at High may be exported only to High users, i.e., users at the Administrator Interface and the High LAN Interface. Note: This rule relies on the validity of the Secure Usage Assumptions in Chapter 3.

Information Flow Security Policy

Information Integrity Rules

A connection may be classified as either *recoverable* or *non-recoverable*. Recoverable connections ensure no loss of data in the case of failure.

More specifically, for every recoverable connection, the sequence of data messages successfully delivered by the NP over the High LAN Interface shall be a prefix of the sequence of data messages successfully received by the NP over the Low LAN Interface.

For every non-recoverable connection, the sequence of data messages successfully delivered by the NP over the High LAN Interface shall be a subsequence of the sequence of data messages successfully received by the NP over the Low LAN Interface. A subsequence of a sequence S is simply the prefix of S with arbitrary members missing.

Pump Protocol

This protocol is specified in detail in [5].

SoF-Basic

A level of the NP strength of function where analysis shows that the function provides adequate protection against casual break of TOE security by attackers possessing a low attack potential.

SoF-High

A level of NP strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized break of NP security by attackers possessing a high attack potential.

SoF-Medium

A level of NP strength of function where analysis shows that the function provides adequate protection against straightforward or pointed break of TOE security by attackers possessing a moderate attack potential.